Dialogic®

Dialogic® PowerMedia™ XMS

Installation and Configuration Guide

March 2013 05- 2704-005

www.dialogic.com

Copyright and Legal Notice

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Inc. and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see http://www.dialogic.com/company/terms-of-use.aspx for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Inc. at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements**.

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, ControlSwitch, I-Gate, Mobile Experience Matters, Network Fuel, Video is the New Voice, Making Innovation Thrive, Diastar, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, NaturalAccess and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Table of Contents

Revision History

Revision	Release Date	Notes
05-2704-005	March 2013	System: Updated with details on Time page. VXML: Updated with clarification that VXML is audio-only.
05-2704-004	February 2013	Updates to support PowerMedia XMS Release 2.0. Configuring PowerMedia XMS: Added new MRCP Client, VXML, RESTful API, and HTTP Client menus. Removed the Diagnostics menu. System: Added new Upgrade and NFS Mount Points pages. MRCP Client: Added new section. HTTP Client: Added new section. VXML: Added new section. MSML: Added new configuration parameters. RESTful API: Added new section. System Level Troubleshooting: Updated with log file details for troubleshooting. XMSTool RESTful Utility: Updated download instructions in the Starting XMSTool section. Removed start command from the Demo/Simple Mode section. Updated the Basic Operation and Commands and Additional XMSTool Commands sections.
05-2704-003	August 2012	RPM Method: Added information about the perl-core package. XMSTool RESTful Utility: Updated the Starting XMSTool and Demo/Simple Mode sections.
05-2704-002	July 2012	Updates to support PowerMedia XMS Release 1.1. This is a 64-bit only release. RPM Method: Added new section. Configuring PowerMedia XMS: Added new Time and Backup/Restore pages to Systems menu. Added new Network menu. Renamed the Interface menu to Protocol. XMSTool RESTful Utility: Added new section.
05-2704-001	March 2012	Initial release of this document.
Last modified: March 2013		

Refer to www.dialogic.com for product updates and for information about support policies, warranty information, and service offerings.

1. Welcome

This Installation and Configuration Guide provides information about installing, configuring, administering, and maintaining the Dialogic® PowerMedia™ Extended Media Server (also referred to herein as "PowerMedia XMS" or "XMS").

2. Installation Process

Overview of Installation Process

This section provides the steps required to successfully install PowerMedia XMS. There are two installation methods available:

- ISO Method
- RPM Method (used for a CentOS or RHEL installation)

System Requirements

Regardless of the installation method used, the recommended **minimum** and **recommended** system requirements are as follows:

Item	Requirement
Hardware	Intel Architecture-based server
Operating System	**Note:** 32-bit operating systems are not supported. Community ENTerprise Operating System (CentOS) 6.2 or higher (provided with the installation) Red Hat Enterprise Linux (RHEL) 6.2 or higher **Note:** The *perl-core-5.10.1-xxxxx.x86_64.rpm* is required if using the RPM Method.
Processor	**Minimum:** Intel Xeon E5420 Quad-Core (2.50 GHz, 1333 MHz FSB, 80W) **Recommended:** Intel Xeon X5650 Dual Hex-Core (2.66 GHz, 1333 MHz FSB) or better for performance systems
Ethernet	Dual 1000Base-TX (RJ-45)
Memory	**Minimum:** 4 GB RAM **Recommended:** 8 GB RAM or higher
Storage	60 GB HDD
Note: The recommended server configuration is applicable for higher density audio solutions of 1500 or greater sessions, video transcoding solutions, or solutions utilizing virtualization.	

ISO Method

The ISO installation method is a complete system installation that includes the CentOS, OS optimizations, and PowerMedia XMS software. The ISO can be installed from a DVD drive or to a Virtual Machine.

Note: ISO install is now 64-bit only.

This installation requires the following steps which will be described in detail below:

1. Download a single .ISO file which contains CentOS and all required PowerMedia XMS software.
2. Burn the .ISO image onto a PowerMedia XMS installation DVD.
3. Ensure the target system on which PowerMedia XMS will be installed is connected to your network.
4. Boot the target PowerMedia XMS system from the installation DVD. The DVD will install CentOS 6.2 operating system and required software.

   Caution: The PowerMedia XMS installation will reformat the system hard drive.
5. Perform licensing and configuration.

Getting and Preparing the .ISO File

CentOS is an Enterprise-class Linux Distribution source that provides a simple method for quickly and easily setting up a PowerMedia XMS. Proceed as follows:

1. Download a single .ISO file which contains CentOS and PowerMedia XMS packages. Go to http://www.dialogic.com/products/media-server-software/xms for information about downloading the .ISO file.
2. Using a DVD drive that has write capabilities, along with the appropriate DVD burning software, burn the .ISO image onto a bootable DVD.

Note: A bootable DVD must be created from the downloaded ISO file rather than simply copying the file to the DVD.

Installing the Operating System from the DVD

Caution: This installation will erase all data on the system and reformat your hard drive.

Once the bootable DVD is created, proceed as follows:

1. Insert the bootable DVD in the system drive on which the installation will be done and boot the system from the DVD.
2. Press **Enter** at the boot prompt.

Note: Do not use any other boot options or the automatic installation will not take place.

The installation requires little interaction. The main task is setting up the IP characteristics for the PowerMedia XMS. The IP characteristics are set at the start of the installation using a text-based setup tool and are handled as follows:

- The default setting is to set up an Ethernet interface (eth0) to receive its addresses via DHCP. With this option, it is necessary that PowerMedia XMS be installed in an environment that provides a networked DHCP server to provide it with an IP address.
- Eth0 may also be given a static IP address. This option is preferable when setting up a server. Set the IP address, Netmask and Gateway, as well as the DNS server address if desired.

Once the IP characteristics are complete, the remainder of the installation is "hands off". Once the CentOS install reaches the final screen, click **Reboot** to complete the installation process.

Note: Be sure to remove the installation DVD before the final reboot is done.

RPM Method

The stand-alone RPM installation method is used for installing PowerMedia XMS on existing Linux installations. Instead of an .ISO file, the RPM distribution of PowerMedia XMS uses a gzipped tar file (.tgz). The .tgz file is extracted to a directory on the machine where the PowerMedia XMS will be installed. The PowerMedia XMS installation script is run from that directory.

The *perl-core-5.10.1-xxxxx.x86_64.rpm* package is required on the system before running the PowerMedia XMS installation script. The perl-core package is a standard package that is part of the RHEL/CentOS distribution and is normally automatically installed on virtually all systems when the operating system is installed using one or more of the RHEL/CentOS predefined package groups. However, in the case where you manually select each individual package in a RHEL/CentOS operating system installation (for example, when using a kick start file), you must ensure that the *perl-core-5.10.1-xxxxx.x86_64.rpm* is included in the list of packages. It can be installed on an RHEL or CentOS system using "yum install perl-core".

The PowerMedia XMS installation script automatically installs any prerequisite operating system packages (other than perl-core) required by the PowerMedia XMS installation script if the yum utility is used and configured to access either the operating system installation DVD or online package repositories such as RHN. If yum is not available on the system, the PowerMedia XMS installation script will print to the installation log (default: *xms_install.log*). That log contains a list of prerequisite operating system packages required to be manually installed by the user before re-running the PowerMedia XMS installation script.

Note: The default PowerMedia XMS configuration uses the following ports:
tcp: 22, 80, 81, 443, 5060, 15001
udp: 5060, 49152-53152, 57344-57840

Ensure that your PowerMedia XMS system firewall is configured accordingly.

RPM Installation and Script Options

Proceed as follows to complete the RPM installation method:

1. Extract the gzipped tar file to a directory of your choice. The chosen directory will contain a subdirectory named dialogic_xms_x.xx.xxx where x is a version number.
2. Run *xms_install.pl* with the desired options from the subdirectory above.

The options available are:

- cfg-xxx Options
- Mode Options
- General Options

cfg-xxx Options

These are platform configuration options. They include:

```
  --cfg-selinux       Disable selinux (default: ask)
  --cfg-hosts         Configure /etc/hosts file (default: ask)
  --cfg-prereq        Automatically install prerequisite OS packages (default: ask)
  --cfg-https         Backup and replace https settings (default: ask)
```

For example, to install PowerMedia XMS and automatically configure the /etc/hosts file,use:

```
xms_install.pl  -i --cfg-hosts
```

The –cfg-xxx options can be negated with nocfg-xxxx. For example, if the script is to ignore the /etc/hosts file, use:

```
xms_install.pl  -i --nocfg-hosts
```

Mode Options

```
  -i or --install      Install XMS if no previous version exists (default)
  -u or --update       Update XMS without affecting current configuration
  -r or --remove       Remove XMS
  -t or --test         Test system and report status without installing anything
```

General Options

```
  -y or --yes             Answer yes to all questions
  -h or --help:           Display this message and exit
  -d or --distdir DIR     Directory where the XMS distribution is located
  -l or --log or --nolog  Log (or not) results to a file (default: enabled)
  -f or --logfile FILE    Use FILE as the log filename (default: xms_install.log)
  -v or --verbose         Print detailed progress information (-vv very verbose)
  -q or --quiet           Do not write anything to standard output (implies –y)
```

Note: The --quiet option implies a yes answer to all questions unless --nocfg-xxxx is added to the command.

If errors occur, review the log file for error and warning information. A log file (default: *xms_install.log*) is generated automatically unless --nolog is specified.

When the installation script completes, use your browser to log in to the PowerMedia XMS Console (refer to Login to the Console).

3. Using the PowerMedia XMS Admin Console

Overview of Using the PowerMedia XMS Admin Console

The PowerMedia XMS Admin Console (also referred to herein as "Console") is a secure web-based GUI used to manage PowerMedia XMS. The Console can be reached using a web browser and the PowerMedia XMS IP address.

If DHCP is used to provide the PowerMedia XMS IP address, it will be necessary to access the system to determine the address assigned to it. Shell access to the system may be done either by the terminal used during installation or by secure shell (ssh) access. The "root" user's default password is "powermedia". If you wish to change the password, do so before proceeding.

Note: For stand-alone RPM installations, password modification is not necessary as the installation script does not change the password to "powermedia" as it does with the .ISO install.

CentOS HTTPS Setup for Console Use

Secure HTTP is used to communicate between the administrator's browser and the PowerMedia XMS Admin Console's interface. HTTPS usually requires a security certificate linked to the provider's domain and signed by a trusted third party.

With PowerMedia XMS, it is not possible to provide a certificate tied to any one domain because the PowerMedia XMS is intended to be installed in many different situations by different administrators. For this reason, a "self-signed" (non-verified) certificate is shipped with PowerMedia XMS. The procedure for creating and installing non-verified certificate on CentOS can be found at http://wiki.centos.org/HowTos/Https. The web browser used to access the Console will detect the use of this self-signed certificate and flag it as a security exception.

Access the Console directly using HTTPS by adding the IP address in browser's address space. For example, https://<ip_address_of _eth0>.

Note: If HTTP is used the query will be redirected to HTTPS on port 443.

Accessing the console will trigger a security exception. Handling the security exception depends on the web browser being used. Refer to the following table for instructions when using one of the four most common browsers.

Browser	Security Exception	Action	Comment
Firefox	Connection is not trusted	Understand the Risks/Add Exception/Confirm Security Exception	Security exception remains permanently in effect
Google Chrome	Site's security certificate is not trusted	Proceed Anyway	Security exception will be seen again on starting Google Chrome

Browser	Security Exception	Action	Comment
Internet Explorer	Problem with website's security certificate	Continue	Security exception will be seen again on starting new Internet Explorer window
Safari	Cannot verify identity of the website	Continue	Security exception will be seen again on starting Safari

Recurring security exceptions can be overcome on Google Chrome, Internet Explorer, and Safari. First, add mapping in the "hosts" file:

xms.localhost <xms_server_ip_address>

Next, add the xms.localhost certificate into the Trusted Root Certification Authorities store. Hosts may be found on Linux systems under */etc*, and on Windows systems under *C:\windows\system32\drivers\etc*. This differs depending on the web browser in use.

- **Google Chrome**
  Crossed-out lock and https symbols will be seen when the Console screen is accessed. Click on the **Lock Symbol > Certificate Information > Details > CopytoFile** and work through the Certificate Export Wizard to save the xms.localhost certificate. It can then be imported into Chrome. Use **Tools > Options > Under the Hood > HTTPS-SSL Manage Certificates > Trusted Root Certification Authorities** to import.
- **Internet Explorer**
  A Certificate Error will be seen next to the URL entry. Install the xms.localhost certificate using **Certificate Error > View Certificates > General Tab > Install Certificate** and work through the Certificate Import Wizard. The xms.localhost certificate will end up in the Trusted Root Certification Authorities store.
- **Safari**
  A pop-up warning will be seen on accessing the Console. Install the xms.localhost certificate using **Show Certificate > Install Certificate** and work through the Certificate Import Wizard. The xms.localhost certificate will end up in the Trusted Root Certification Authorities store.

Guidelines for Installing a Permanent Security Certificate

A permanent, publicly accessible PowerMedia XMS should use a valid certificate from a trusted certificate authority. A large number of vendors provide security certificates. Use the following guidelines when installing a certificate from your preferred vendor:

- Upon installation, the fully qualified domain name of the PowerMedia XMS is xms.localhost. The self-signed certificate supplied with PowerMedia XMS uses this name. Therefore, change the server name/domain.
- The web server used for the Console is Apache, version 2.2.15. There is also a lighttpd server on the system, but it is used for the RESTful interface to PowerMedia XMS and can be ignored.
- Secure HTTPS access is provided by mod_ssl, the OpenSSL interface to Apache.

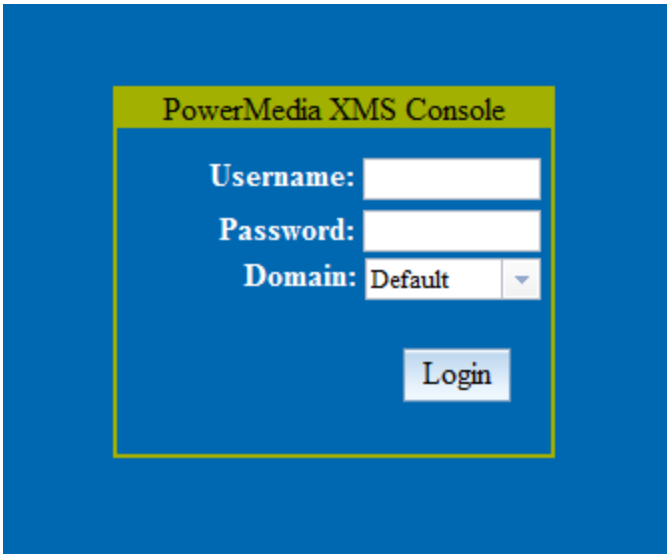
- The configuration file for the SSL Virtual Host is */etc/httpd/conf.d/ssl.conf*. Entries to modify when a purchased certificate is activated include:
  – SSLCertificateFile
  – SSLCertificateKeyFile
  - SSLCertificateChainFile

Login to the Console

Proceed as follows to connect to the Console.

1. Launch your web browser. In the address field, enter the IP address in URL format. For example, https://<ip_address_of_eth0>.

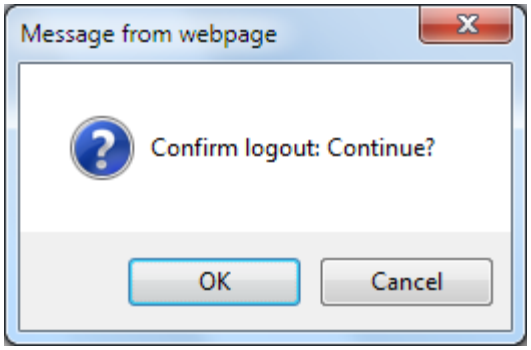
   The Login page appears.



2. Enter "superadmin" for the **Username** field and "admin" for the **Password** field. The superadmin user allows access to all configuration functions available on the Console.
3. Click **Login**. After user information is authenticated, you are logged on to the initial **General** page of the **Systems** menu.
4. The Console is designed as follows:
   - The page title at the top.
   - A side-bar menu used for navigation.
   - One or more tabs at the top that contain more information for each side-bar menu item.
   - A display area for viewing and changing data.

The option to log out appears on each screen in the upper right-hand corner.

1. Click **logout**. Depending on your browser, a popup similar to the following appears to confirm logout.



2. Click **Cancel** to return to the Console.
3. Click **OK** to close the Console session and return to the Console's Login page.

4. Configuring PowerMedia XMS

Overview of Configuring PowerMedia XMS

PowerMedia XMS configuration and operation is done though the Console. This section provides details about the Console's functionality.

Note: The functionality displayed on the side-bar menu will differ between the two operation modes, MSML and Native.

The side-bar menu contains the following choices:

- System
- Network
- License
- MRCP Client
- HTTP Client
- VXML
- MSML
- RESTful API
- Protocol
- Codecs
- Routing
- Tones
- Media
- Options
- Downloads

System

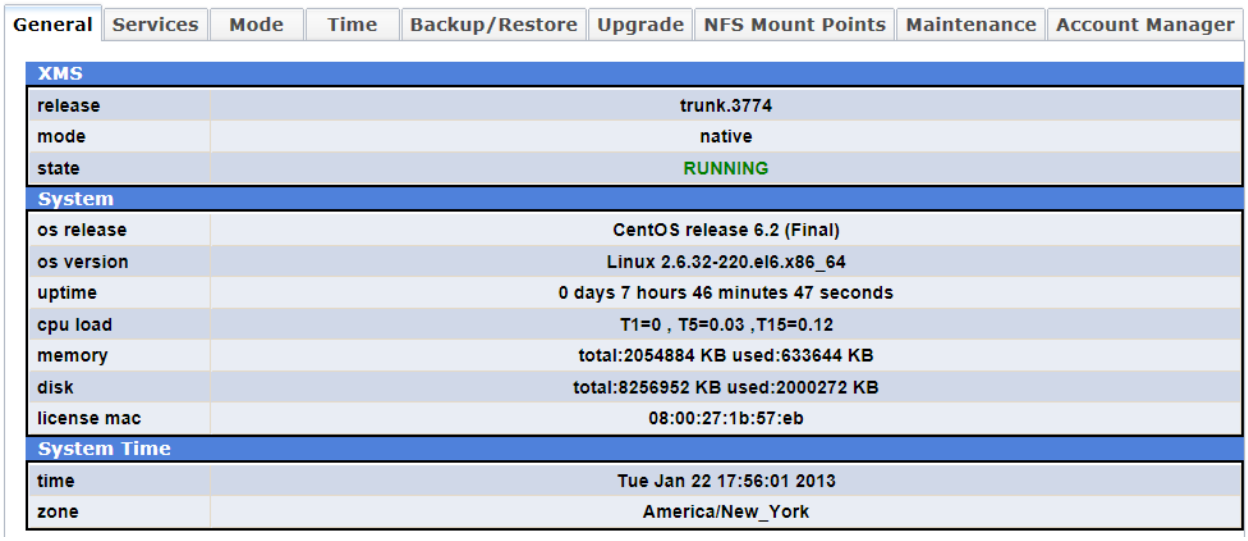
The **System** menu provides system information about the PowerMedia XMS you have logged into.

The following pages are accessible via tabs that provide additional options:

- General
- Services
- Mode (visible only to superadmin)
- Time
- Backup/Restore
- Upgrade
- NFS Mount Points
- Maintenance
- Account Manager

General

When you log in, the **General** page of the **System** menu is displayed. On this page, PowerMedia XMS operation can be verified.



The following information is provided:

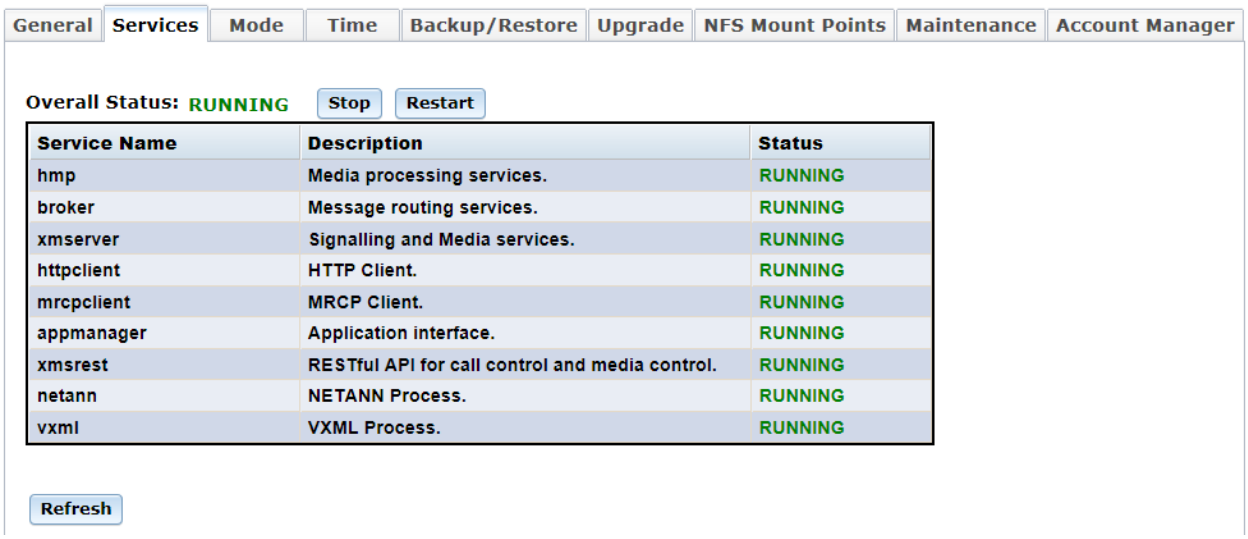
Item	Description
XMS	Displays release name, mode, and state of the PowerMedia XMS.
System	Displays the operating system release and version, and provides the uptime, CPU load, memory, and disk space used. It also displays the MAC address used for licensing.
System Time	Displays the current time and time zone.

Services

The option to stop or start services is available from the **Services** page of the **System** menu. You can also view which services are currently running.

To stop services, click **Stop**. The **Overall Status** will change from running to waiting to stop services. Services are stopped when the column changes to stopped and the **Stop** button changes to **Start**.

To start services, click **Start**.



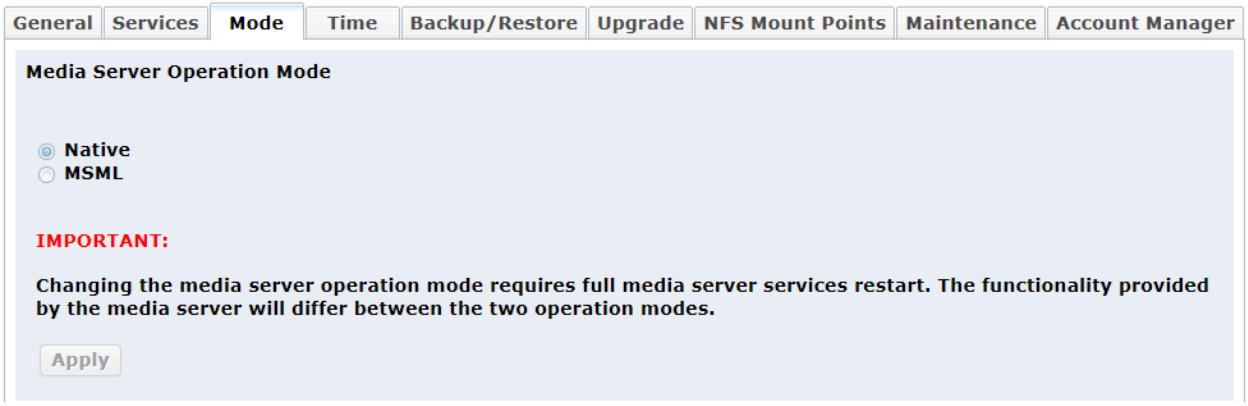
Mode

The **Mode** page of the **System** menu displays the operation mode of the PowerMedia XMS, which defaults to MSML mode.

There are two operational modes:

- MSML (Media Server Markup Language for PowerMedia XMS) is used for application control.
- Native mode means that application control is desired via a RESTful (Representational State Transfer) application.

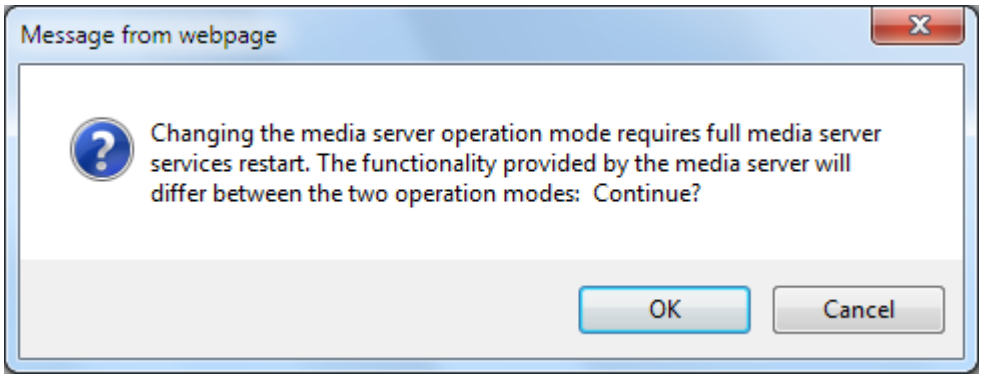
Note: The Mode page is present only when logged in as superadmin.



To switch between modes:

1. Select the **Mode** page.
2. Click the desired radio button, **Native** or **MSML**.

3. Click **Apply**. The following popup appears:

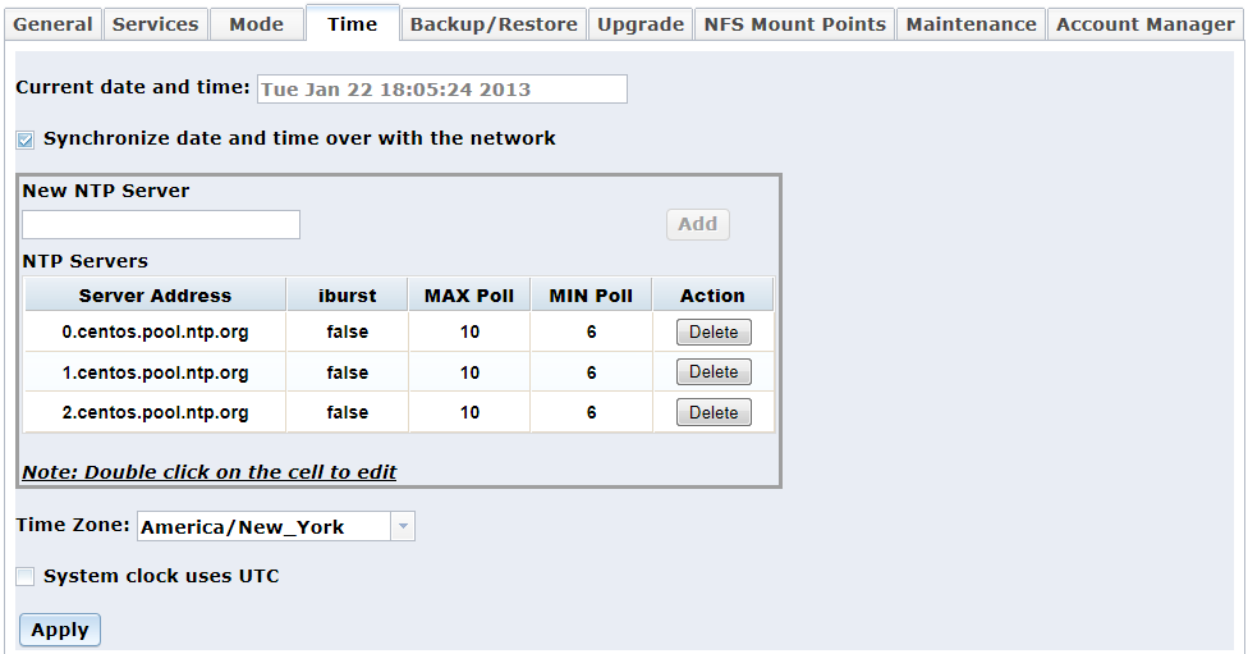


4. Click **OK** to continue or Cancel to return to the **Mode** page.

Note: Once OK is clicked, PowerMedia XMS will stop and restart automatically.

Time

The **Time** page of the **System** menu displays the System's current date and time, time zone, and allows an administrator to change date and time parameters.



The following information is provided:

Item	Description
Synchronize date and time over with the network	Keep the system's date and time synced using Network Time Protocol (NTP). Otherwise, allow the date/time to be manually set.
Server Address	Name or IP address of NTP server.

Item	Description
iburst	When the server is unreachable and at each poll interval, send a burst of eight packets instead of the usual one. This is designed to speed the initial synchronization acquisition.
MAX Poll	Maximum poll interval for NTP messages, in seconds, to the power of two.
MIN Poll	Minimum poll interval for NTP messages, in seconds, to the power of two.
System clock uses UTC	Keep the system's hardware clock in UTC/GMT or local time.

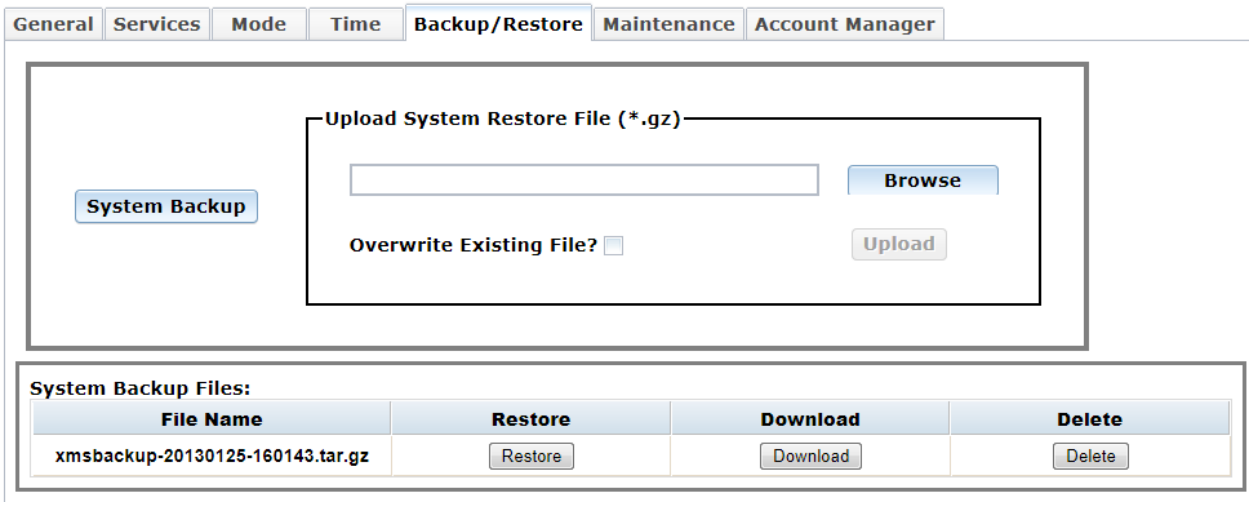
If the **Synchronize date and time over with the network** option is not selected, the date and time may be set manually to the desired value. Otherwise, it provides the option to add or delete NTP servers. NTP servers may be added, deleted, or edited. To edit the NTP servers, double-click on the cell to make changes.

The system's **Time Zone** may be changed using the drop-down menu, and the system's hardware clock mode (UTC/GMT or local time) may be selected.

Note: System services must be stopped before any changes made on this screen are applied.

Backup/Restore

The **Backup/Restore** page of the **System** menu provides the option to perform system backup or restore configurations.



System Backup

Perform the following steps to create a system backup:

1. Click **System Backup** to create a system backup file.
2. Once created, the system backup file will be listed in the **System Backup Files** section.

Restore Backup

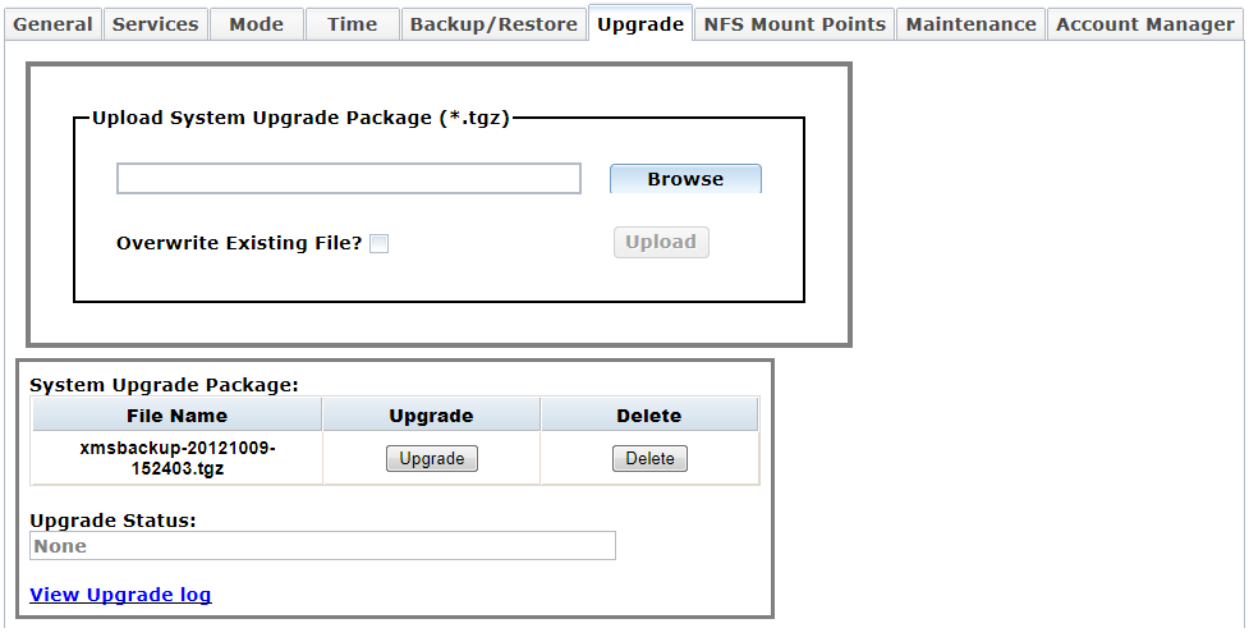
Perform the following steps to restore a system backup:

1. Click **Browse** from the **Upload System Restore File** section to access a system backup file that has been downloaded.
2. Once you select the system back file, click **Upload**. After the upload completes, the system backup file will be listed in the **System Backup Files** section.
3. Locate the appropriate system back file and click **Restore**.

Note: If there is already a system backup file listed in the **System Backup Files** section, you can click **Restore** on the appropriate system backup file.

Upgrade

The **Upgrade** page of the **System** menu provides the option to upgrade the system by uploading a system upgrade package.



System Upgrade

Perform the following steps to upgrade the system:

1. Click **Browse** from the **Upload System Upgrade Package** section to access a system upgrade package file that has been downloaded.
2. Once you select the system upgrade package file, click **Upload**. After the upload completes, the system upgrade package file will be listed in the **System Upgrade Package** section.
3. Locate the appropriate system upgrade package file and click **Upgrade**.

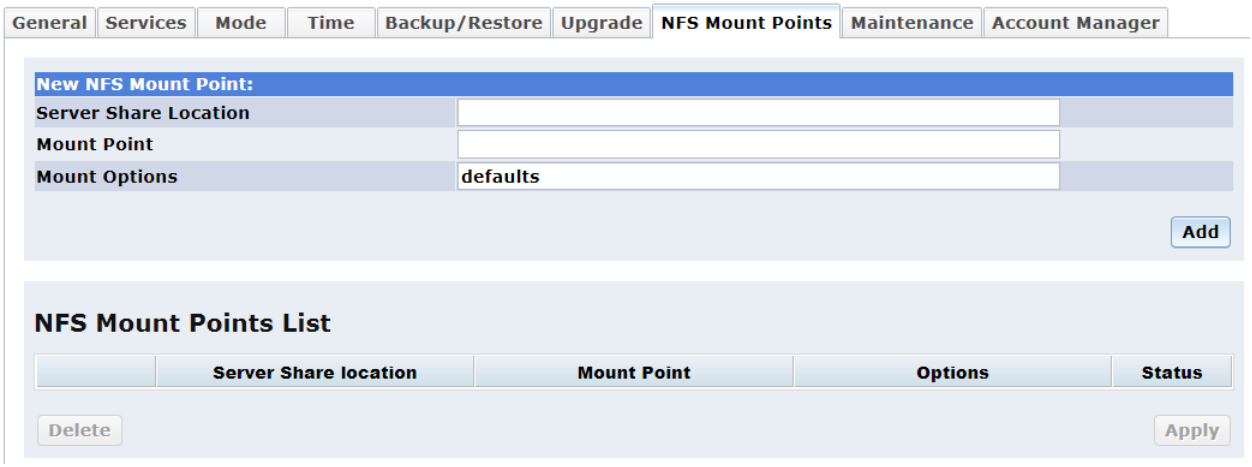
Note: If there is already a system upgrade package file listed in the **System Upgrade Package** section, you can click **Upgrade** on the appropriate system upgrade package file.

NFS Mount Points

The **NFS Mount Points** page of the **System** menu allows Network File System (NFS) version 4 file systems, offered by external servers, to be mounted on PowerMedia XMS.

Resources used by PowerMedia XMS, such as media files or VXML scripts, may be kept on an external file server, but may be needed by for handling calls. NFS mount will allow for this.

The NFS server must be correctly configured to allow mounting of its file system on the PowerMedia XMS NFS client. This is outside the scope of this document.



Adding a Mount Point

Multiple mounts may be defined. Each is individually added, and will then be displayed in the **NFS Mount Points List** section.

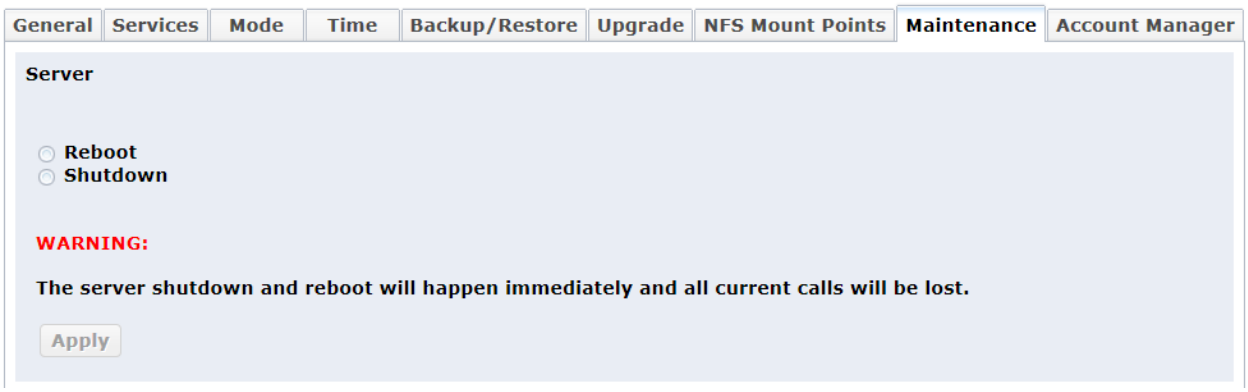
1. Enter the **Server Share Location**. Typically, this will consist of the IP address of the server, followed by a colon, followed by a location in the exported file system. For example, if the NFS server exports */var/lib/media/en-US*, the **Server Share Location** 192.168.1.100:/ will mount the contents of the en-US directory at the given **Mount Point**.
2. Change the default **Mount Options** ("defaults") if desired. See the MOUNT OPTIONS section of the nfs (5) man page for other possible settings.
3. Enter the **Mount Point**. This will be a directory in the PowerMedia XMS file system. A typical example would be */mnt*. The **Mount Point** must already exist in the PowerMedia XMS file system or the mount operation will time out. It may be necessary to manually add mount points by logging into PowerMedia XMS using ssh.
4. Click **Add** to execute the mount operation. The mounted file system is activated.

Deleting a Mount Point

Mounted file systems are deleted by checking off the file system row in the **NFS Mount Points List** section and clicking **Delete**. The file system will be unmounted and the row will be deleted from the list.

Maintenance

The **Maintenance** page of the **System** menu page provides the option to reboot or shut down the PowerMedia XMS.



To reboot, click the **Reboot** radio button, and then click **Apply**.

To shut down, click the **Shutdown** radio button, and then click **Apply**.

Note: Once you click **Apply**, the reboot or shut down action occurs immediately and all current calls are lost.

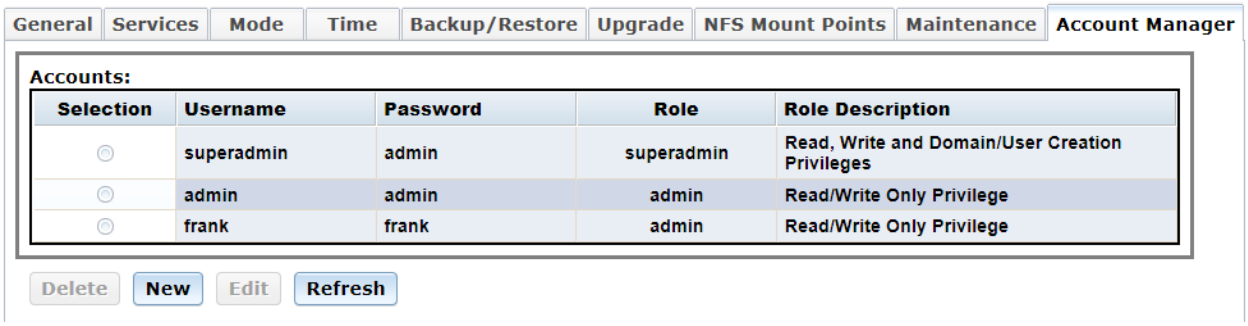
Account Manager

The **Account Manager** page of the **System** menu provides options to manage accounts.

The PowerMedia XMS supports two access levels:

- Superadmin – able to change the configuration of the PowerMedia XMS and execute administrative tasks.
- Admin – able to monitor the PowerMedia XMS, but cannot change configurations or execute administrative tasks.

Commands that are only available to administrators are noted as such. All other commands are usable by both operators and administrators.



Create a New User

Follow the instructions below to create a new user and then log in using the new accounts username and password. Up to 20 new user accounts can be created.

The account being created will have configure and provisioning permissions but will not have administrative permissions.

1. Click **New**. The **New Account Editor** dialog box will appear.
2. Enter a Username and Password in the corresponding **Username** and **Password** fields. The account being set up is a user account and not an administrative account.
3. Click **Commit** and the object and the new user will get created under the admin icon in the configuration tree.

4. Once the account has been created, log on to the newly created account.
5. Log off by clicking on **logout** in the upper right-hand corner of the page.

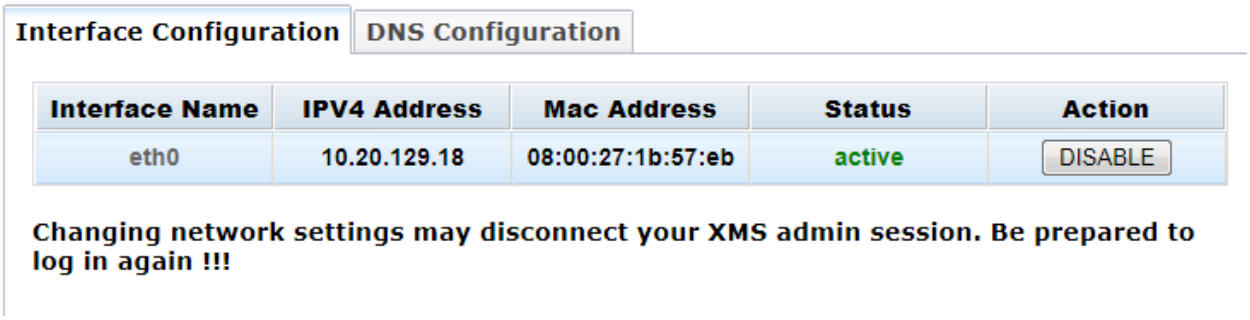
Network

From the **Network** menu, you can view and change the **Interface Configuration** and the **DNS Configuration**.

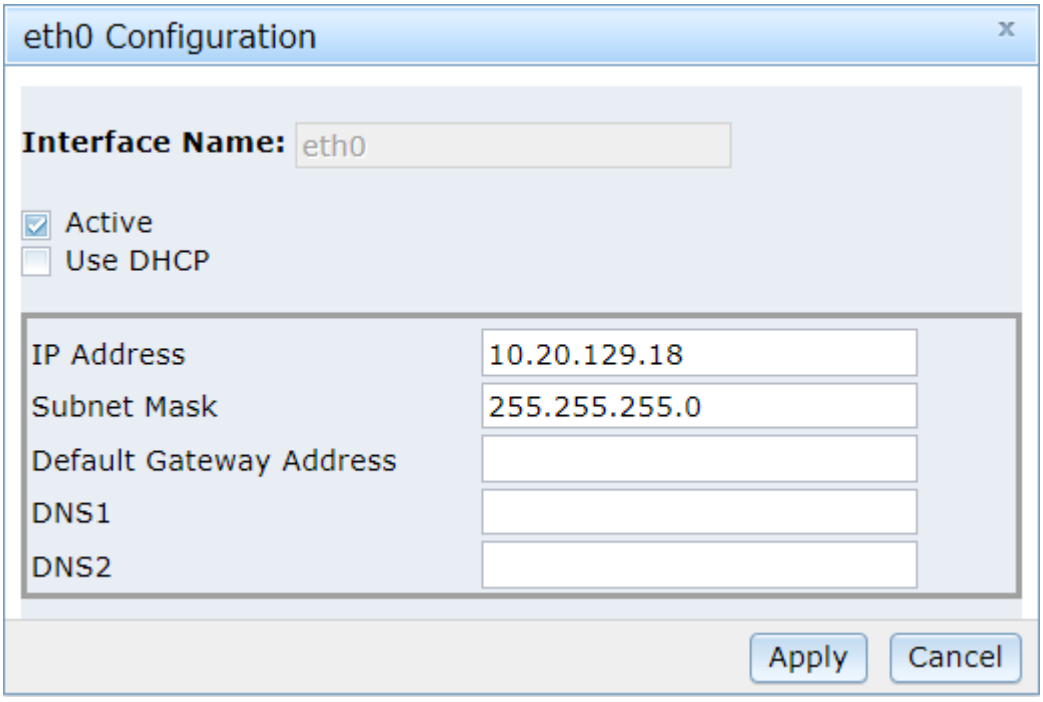
Note: This **Network** menu applies to system network settings, while the **Protocol** menu applies to PowerMedia XMS network settings.

Interface Configuration

The **Interface Configuration** page is used to configure the IPV4 network device. The table displays the number of network devices and their IPV4 configuration in the system.



Click **Interface Name** to display the **Active** network device configuration dialog box.

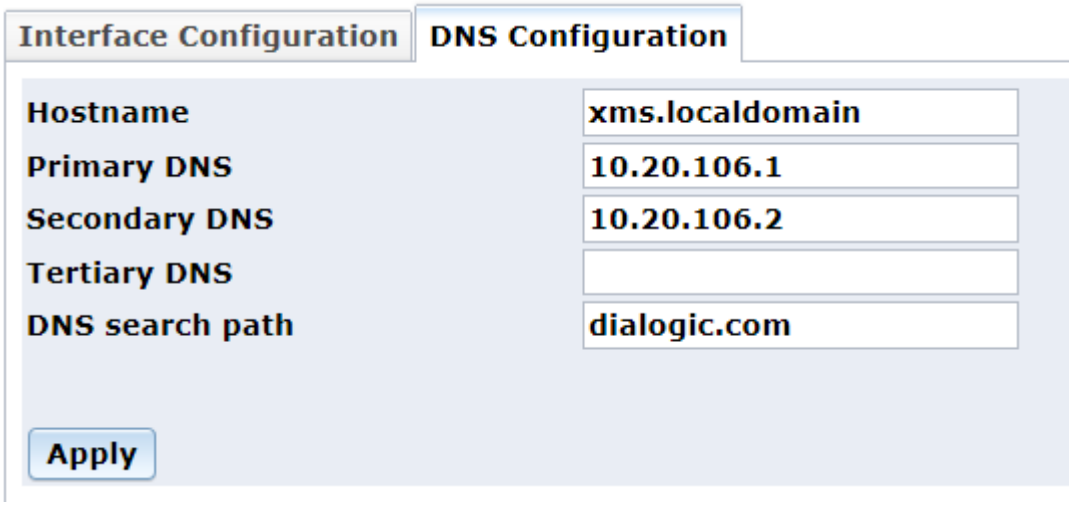


If the **Use DHCP** check box is not checked, the static IPV4 configuration is provided.

Click **Apply** to save changes.

DNS Configuration

The DNS client is configured using the **DNS Configuration** page.



Proceed as follows to configure the **DNS Configuration** parameters:

1. In the **Hostname** field, enter the name of the host machine.
2. In the **Primary DNS** field, enter the Primary DNS server IP address.
3. In the **Secondary DNS** field, enter the Secondary DNS server IP address.
4. In the **Tertiary DNS** field, enter the Tertiary DNS server IP address.
5. In the **DNS search path** field, enter the search path for DNS servers.
6. Click **Apply** to save changes.

License

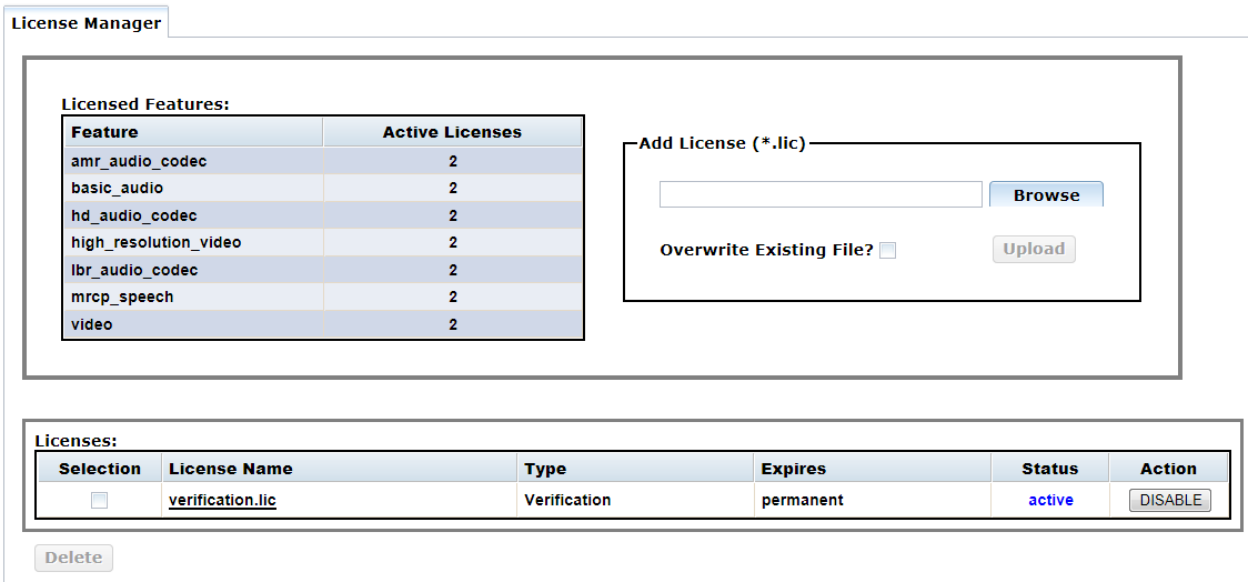
From the **License** menu, you can view the **License Manager** page.

The **License Manager** page provides the options to view available licenses, browse for new licenses, and add, activate or delete licenses. The primary method of activation is interactive through use of the Console. To activate your license, you must have access to the license file from the License Certificate or via an email from Dialogic.

Note: The PowerMedia XMS comes with a two-port audio/video license to get started. The license name is *verification.lic*. When another license is enabled, the Verification License automatically becomes inactive.

The **License Features** section of the **License Manager** page provides a view of license features and the number of active licenses in use. The **Licenses** section provides a list of licenses available on PowerMedia XMS. To toggle between disabling and enabling the license, click the check box to the left of the license name to select a license, and then click **ENABLE** or **DISABLE** in the **Action** column.

Note: Mixing verification, trial, and permanent licenses are not allowed, however, multiple purchased licenses can be active at the same time.



Add a License

Perform the following steps in the **Add License** section to add a license:

1. Click **Browse** to access available licenses that have been downloaded to the PowerMedia XMS on which your web browser is running.
2. Once you select the license, click **Upload**.
3. Restart services using the **System > Services** page to apply changes to the licensing.

Delete a License

Perform the following steps in the **Licenses** section to delete a license:

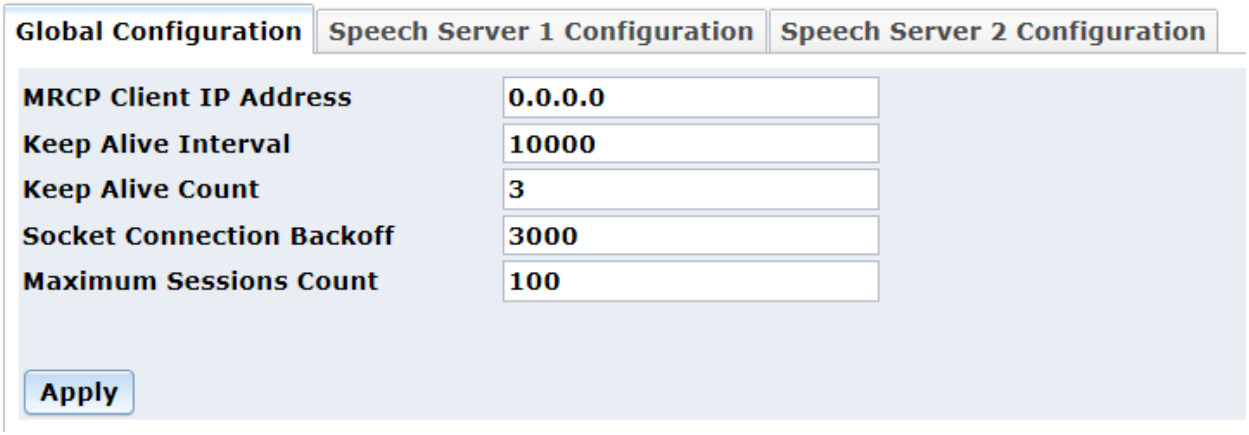
1. Click in the check box to the left of the license you wish to delete.
2. Once you select the license, click **Delete**.
3. Restart services using the **System > Services** page to apply changes to the licensing.

MRCP Client

The Media Resource Control Protocol (MRCP), accessible only through VXML, is used by PowerMedia XMS as an interface to Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) systems. MRCP provides an easy way to build voice user interfaces, allowing a grammar to be built for speech input and providing a way to easily translate text into voice prompts without reading and recording them.

Global Configuration

The **Global Configuration** page is used to configure the MRCP Client.



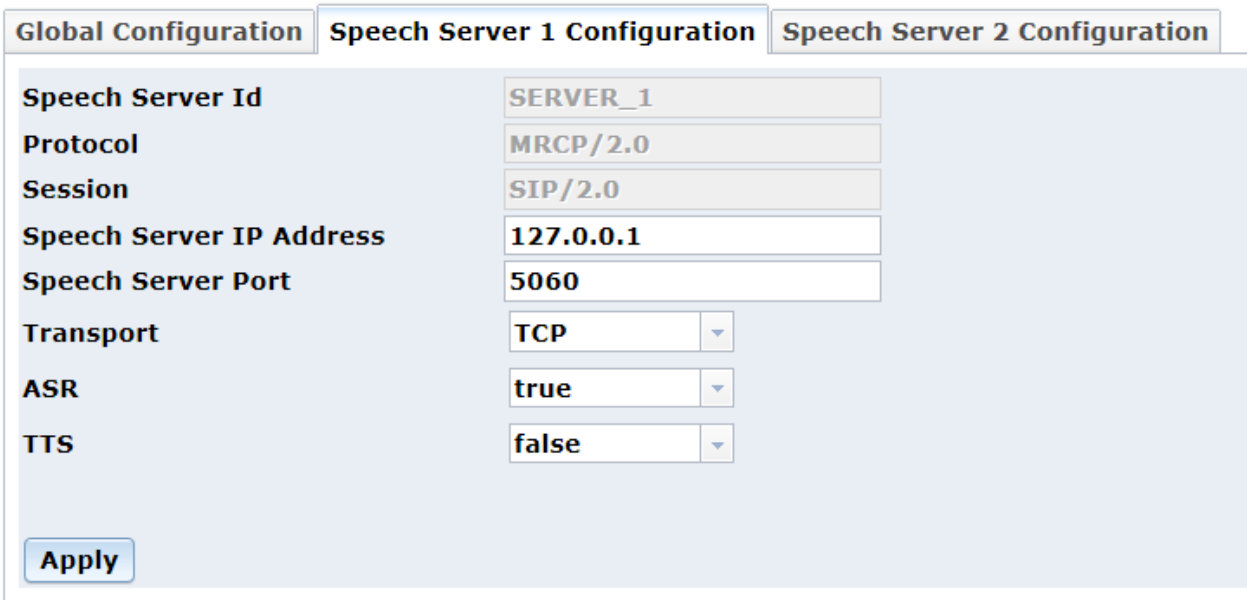
Proceed as follows to configure the **Global Configuration** parameters:

1. In the **MRCP Client IP Address** field, enter the local IP Address to be used for the MRCP Client.
2. In the **Keep Alive Interval** field, enter the keep alive interval for connection with speech server.
3. In the **Keep Alive Count** field, enter the keep alive count for connection with speech server.
4. In the **Socket Connection Backoff** field, enter the socket connection backoff - delay before TCP reconnection.
5. In the **Maximum Sessions Count** field, enter the maximum number of MRCP sessions supported.

   Note: If the MRCP server contracted by the MRCP client uses both ASR and TTS, then the **Maximum Sessions Count** field on the client screen has to be set to two times the number of desired active sessions. This is because ASR and TTS each consume a session, even in the same call.
6. Click **Apply** to save changes.

Speech Server 1 Configuration

The **Speech Server 1 Configuration** page is used to configure the speech server.



The following fields are non-configurable:

- **Speech Server Id** field shows the speech server identification for MRCP.
- **Protocol** field shows the supported protocol version. (Only MRCP/2.0 is supported)
- **Session** field shows the session type supported to establish the MRCP session. (Only SIP/2.0 is supported)

Proceed as follows to configure the **Speech Server 1 Configuration** parameters:

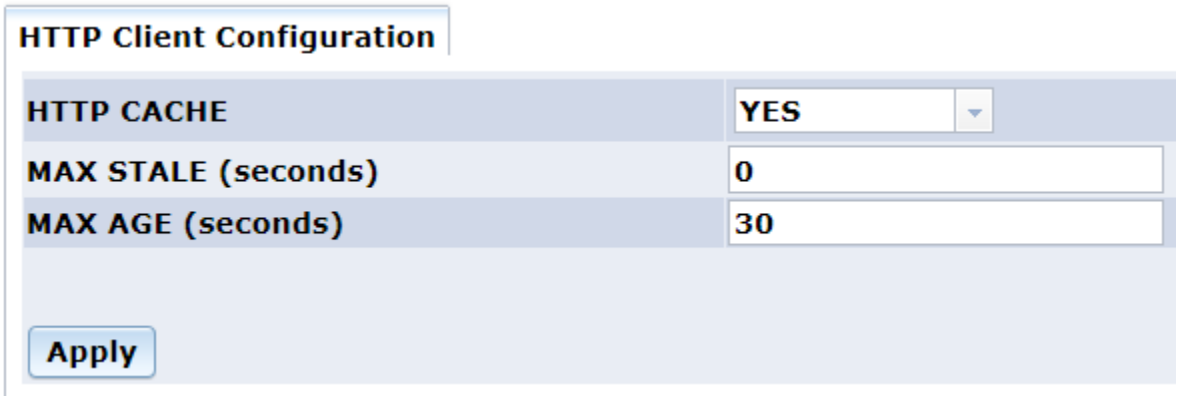
1. In the **Speech Server IP Address** field, enter the IP address of the MRCP server to connect to.
2. In the **Speech Server Port** field, enter the IP port of the MRCP server to connect to.
3. In the **Transport** field, select UDP or TCP from the drop-down list to indicate the SIP Transport protocol.

   Note: For the SIP usage only. Once the session is established, MRCP uses TCP.
4. In the **ASR** field, select true or false from the drop-down list to enable Speech Recognition for this speech server.
5. In the **TTS** field, select true or false from the drop-down list to enable Text-to-Speak usage for this speech server.
6. Click **Apply** to save changes.

Speech Server 2 is used when customer desires ASR from one speech server and TTS from a different speech server. The **Speech Server 2 Configuration** page contains the same fields as shown on the **Speech Server 1 Configuration** page.

HTTP Client

The **HTTP Client** menu opens to the **HTTP Client Configuration** page which is used to configure cache on the HTTP client.



Proceed as follows to configure the **HTTP Client Configuration** parameters:

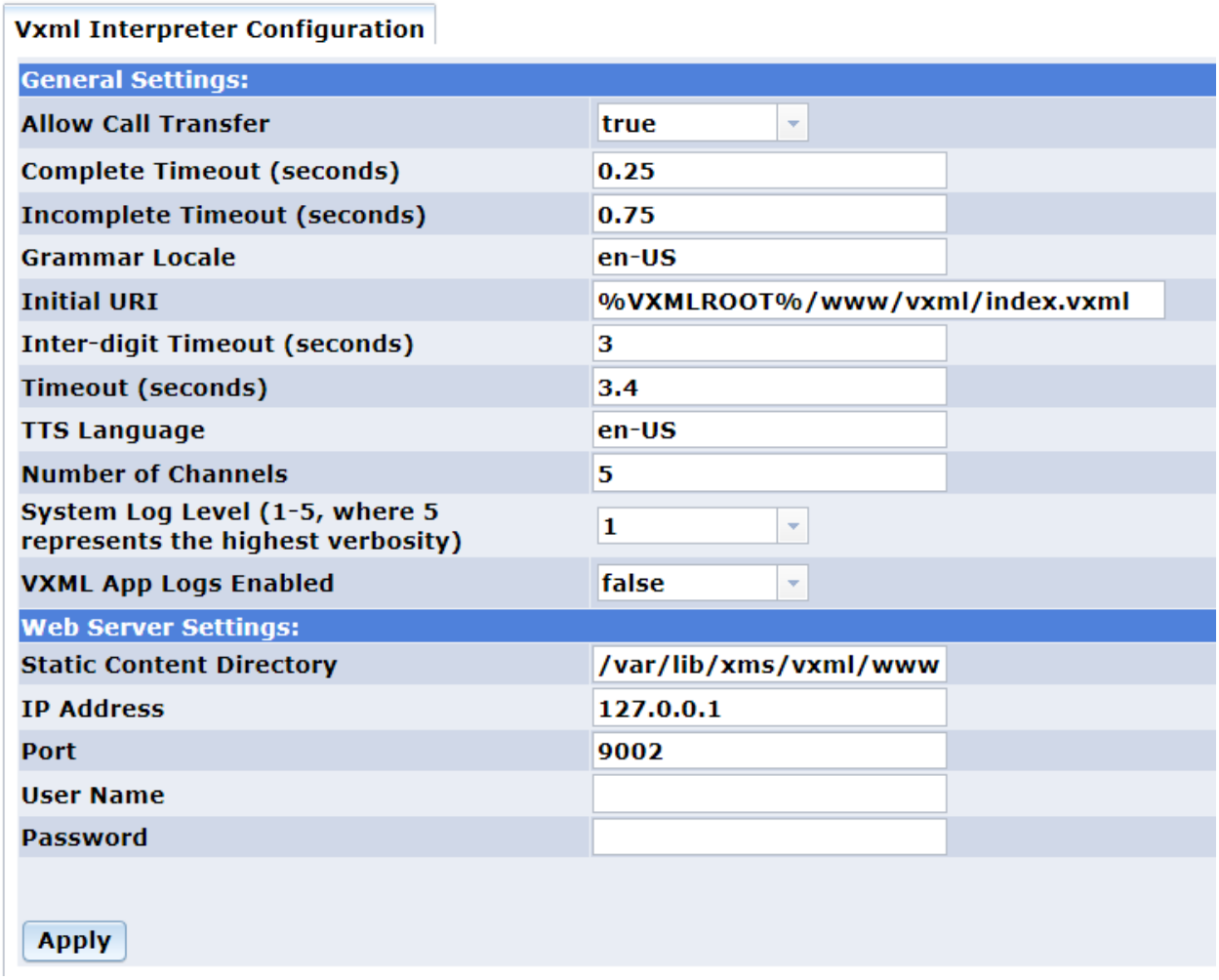
1. In the **HTTP CACHE** field, select **Yes** to enable cache or **No** to disable cache.
2. In the **MAX STALE (seconds)** field, enter the maximum amount of time in seconds that is allowed before a cached file becomes stale.
3. In the **MAX AGE (seconds)** field, enter the maximum amount of time in seconds that a file will be cached.
4. Click **Apply** to save changes.

VXML

Voice Extensible Markup Language (VoiceXML or VXML) is an integral part of PowerMedia XMS Release 2.0. VoiceXML is designed for creating audio-only dialogs that feature synthesized speech, digitized audio, speech recognition and DTMF key input, speech recording, telephony, and mixed initiative conversations.

VXML Interpreter Configuration

The **VXML Interpreter Configuration** page is used to configure **General Settings** for the VXML Interpreter, in addition to the local **Web Server Settings**.



General Settings

Proceed as follows to configure the **General Settings** parameters:

Parameter	Description	Valid Values
Allow Call Transfer	Specifies whether call transfers are allowed. Select TRUE or FALSE from the drop-down list.	True, False
Complete Timeout	Sets the default value of the VoiceXML complete timeout property in seconds.	0.2sec - 10s Default: 0.25s
Incomplete Timeout	Sets the default value of the VoiceXML incomplete timeout property in seconds.	0.2s - 10s Default: 0.75s
Grammar Locale	Sets the default RFC 3066 language identifier to use for grammar.	

Parameter	Description	Valid Values
Initial URI	URI of the initial page to execute when receiving or making a call. The value must be a full URI, because relative URIs are not allowed. Both HTTP and local file URIs are supported. In the latter case, the file:// protocol specifier must precede the path.	
Inter-digit Timeout	Sets the default value of the VoiceXML interdigit timeout property in seconds.	0 - 600s
Timeout	Sets the default value of the VoiceXML timeout property in seconds.	0.05s - 20000s
TTS Language	Default system language. The value should be a language-identifier as per RFC 3066. It can have a particular voice name appended, for example, en-US-Crystal.	
Number of Channels	Number of VoiceXML Interpreter channels to be started. Each channel runs as a separate thread within the VoiceXML Interpreter executable. **Note:** The resources consumed for a channel may not be released immediately after a call is disconnected, because the VoiceXML Interpreter can continue processing dialogs on behalf of a call. To avoid call rejection due to busy resources, it is generally recommended to add twenty percent (20%) more channels than the total concurrent number of calls PowerMedia XMS is expected to handle.	1 - 1024 depending on machine capabilities

Parameter	Description	Valid Values
System Log Level	Minimum severity level that must be assigned to a VoiceXML application log message for it to be written to the VoiceXML Interpreter system log file. **Note:** If the value specified is less than 4, VoiceXML application log messages are not written to the system log file.	1-5, where 5 represents the highest verbosity WARNING ERROR FATAL
VXML App Logs Enabled	Specifies whether to enable VoiceXML application logging. Select TRUE or FALSE from the drop-down list.	True, False

Web Server Settings

Proceed as follows to configure the local **Web Server Settings** parameters:

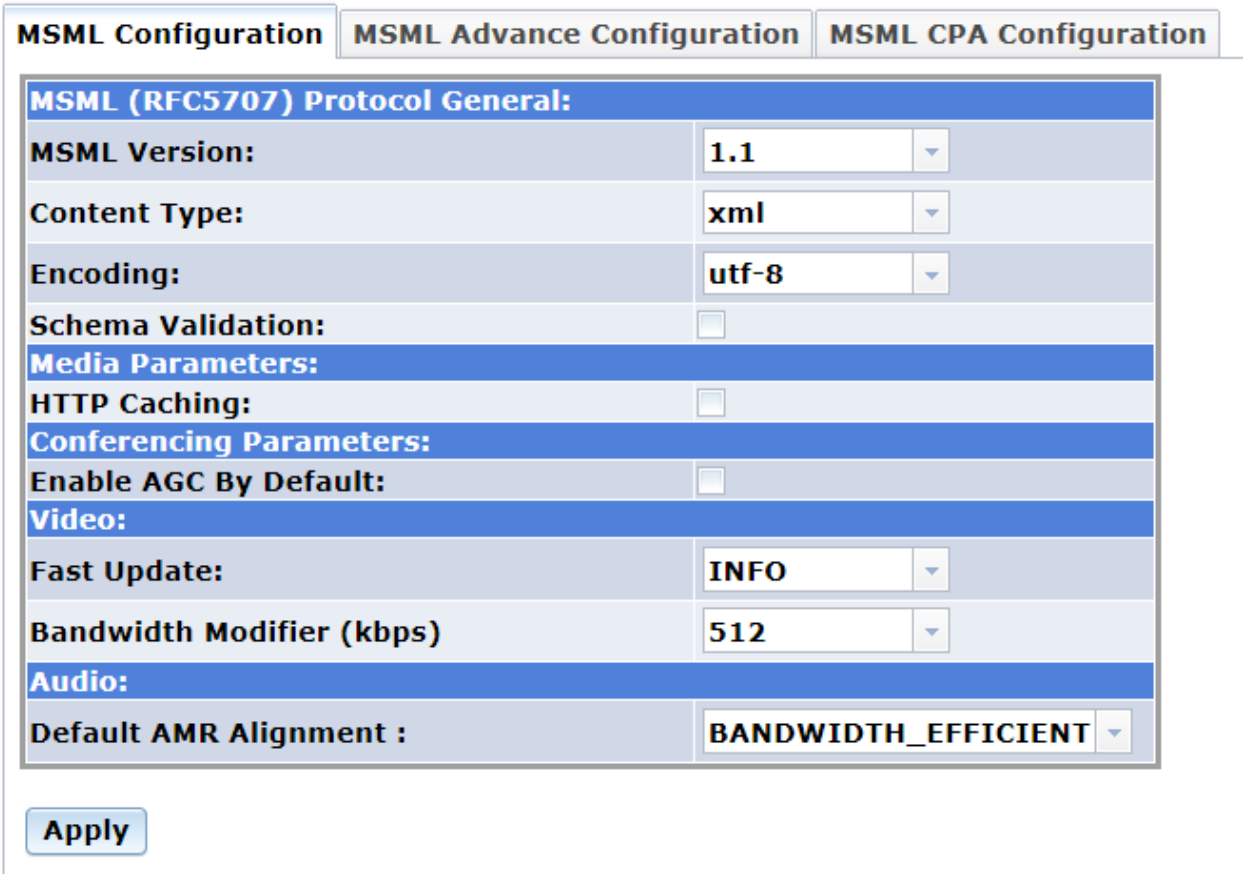
1. In the **Static Content Directory** field, enter the location where the vxml pages are stored.
2. In the **IP Address** field, enter the local IP address to use or LOCALHOST with 127.0.0.1.
3. In the **Port** field, enter the port number.
4. In the **User Name** field, enter the username to login, if any.
5. In the **Password** field, enter the password to login, if any.
6. Click **Apply** to save changes.

MSML

The MSML interface uses SIP INFO messages to send MSML script payloads. The **MSML** menu is viewable only when logged in as superadmin, and is only available when PowerMedia XMS is in MSML mode. When PowerMedia XMS is in Native mode, the **MSML** menu is hidden. Refer to the **Mode** page from the **System** menu for information about switching modes.

The **MSML** menu contains tabbed pages, **MSML Configuration**, **MSML Advance Configuration**, and **MSML CPA Configuration**.

MSML Configuration



Proceed as follows to configure the **MSML Configuration** parameters:

Parameter	Description	Action
MSML Protocol General		
MSML Version	Specifies the MSML version used by the media server.	Use the drop-down list to select the value. Valid values are: • 1.0 • 1.1 (default)
Content Type	Specifies the MSML control package content type.	Use the drop-down list to select the value. Valid values are: • xml (default) • msml-xml
Encoding	Specifies XML encoding.	Use the drop-down list to select the value. Valid values are: • utf_8 (default) • us_ascii

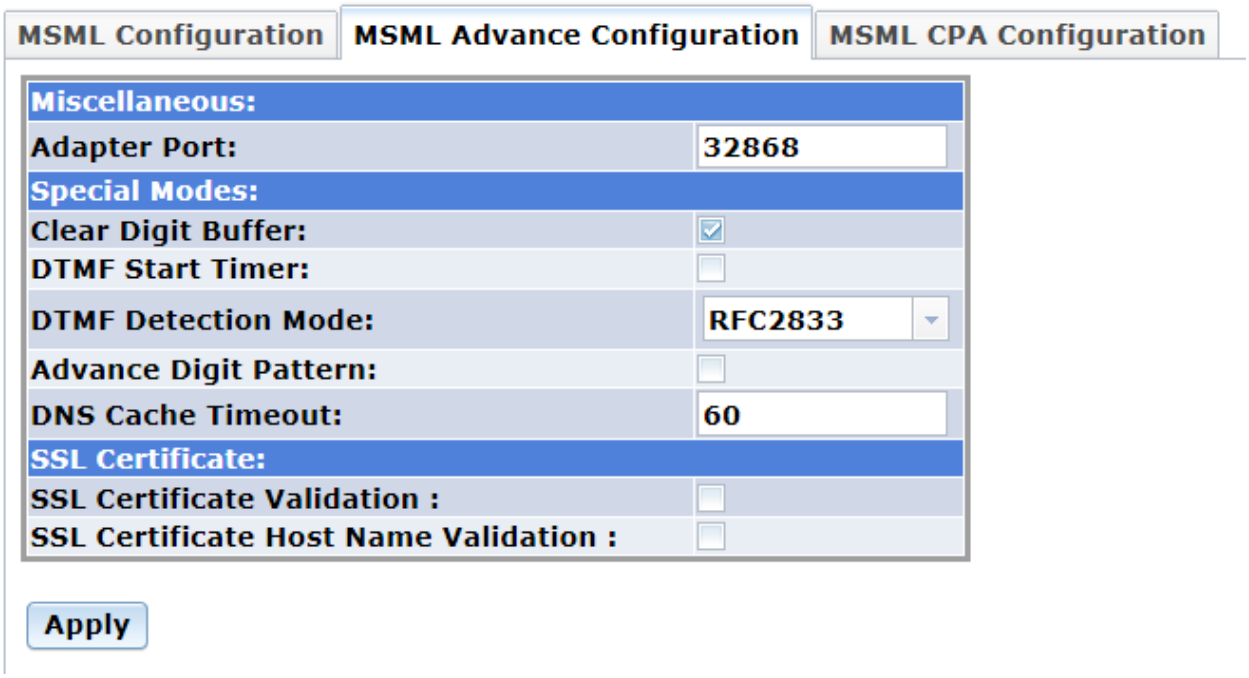
Parameter	Description	Action
Schema Validation	Controls activation of the XML validation of the media control message body. Validation is performed based on the *msml.xsd* XML schema definition file. **Note:** This parameter is MIPs intensive and is recommended during application development and troubleshooting, and not for normal operation.	Click the check box to enable or disable. Schema Validation is disabled by default.
Media Parameters		
HTTP Caching	Controls a caching mechanism to improve performance when servicing network and remote file operations.	Click the check box to enable or disable. HTTP Caching is disabled by default (does not perform caching; all network requests result in remote access).
Conferencing Parameters		
Enable AGC By Default	Enables automatic gain control.	Click the check box to enable or disable AGC by default. The default value is disable.
Video		
Fast Update	Specifies the control method for receiving a video fast update request.	Use the drop-down list to select the value. Valid values are: • info (default, request sent in INFO message) • disable
Bandwidth Modifier (kbps)	Specifies the bandwidth modifier in kilobits per second.	Use the drop-down list to select the value. Valid values are 48, 64, 128, 256, 400, 512, 800, 1024, 2048, 4096. The default value is 512 kbps.

Parameter	Description	Action
Audio		
Default AMR Alignment	Specifies the default adaptive multi-rate alignment.	Use the drop-down list to select the value. Valid values are: • BANDWIDTH_EFFICIENT • OCTET_ALIGNED

Click **Apply** to save changes.

Note: The system services must be restarted for the changes to take effect.

MSML Advance Configuration



Proceed as follows to configure the **MSML Advance Configuration** parameters:

1. In the **Adapter Port** field, enter the adapter port which is used for communication between the MSML interface layer and the media engine.
2. To enable **Clear Digit Buffer**, click the check box.
3. To enable **DTMF Start Timer**, click the check box.
4. In the **DTMF Detection Mode** field, use the drop-down list to select the value. Valid values are: **RFC2833** or **IN-BAND**.
5. To enable **Advance Digit Pattern**, click the check box.
6. In the **DNS Cache Timeout** field, enter the number of seconds DNS entry remains in DNS cache. Set it as **0** to disable DNS caching. Set it as **-1** to leave entries in DNS cache forever. Default value: 60.

7. To enable **SSL Certificate Validation**, click the check box to turn on validation and verify that the HTTP server's certificate is signed by the certificate authority (CA) identified in the certificate bundle.
8. To enable **SSL Certificate Host Name Validation**, click the check box to turn on validation and verify that the host name specified in a play/record URI matches the name in certificate's "Common Name" or "Subject Alternate Name" fields.
9. Click **Apply** to save changes.

Note: The system services must be restarted for the changes to take effect.

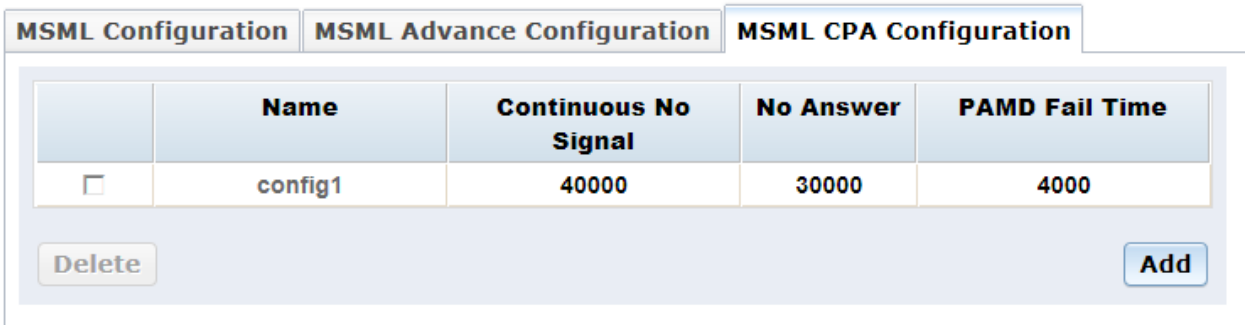
Add a CA Certificate to the CA Bundle

To add a CA certificate to the CA bundle, the user has to append the certificate to the following file on the PowerMedia XMS.

/etc/pki/tls/certs/ca-bundle.crt

Note: As of this release, managing CA certificates through the Console is not supported.

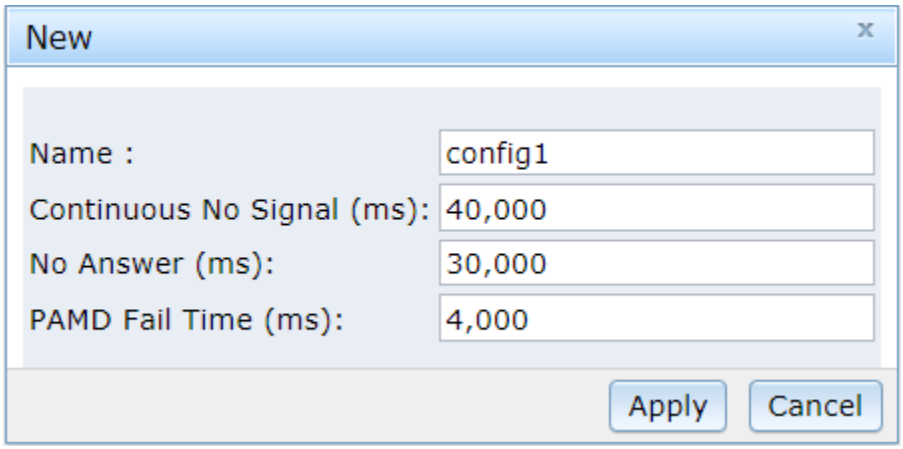
MSML CPA Configuration



Add CPA Configuration

Perform the following steps to add a CPA configuration:

1. On the **MSML CPA Configuration** page, click **Add**. The following dialog box appears:



2. In the **Name** field, enter the name of CPA configuration.

3. In the **Continuous No Signal (ms)** field, enter the maximum time of silence (no signal) allowed immediately after cadence detection begins. Default value: 40,000 ms.
4. In the **No Answer (ms)** field, enter the length of time to wait after first ringback before deciding that the call is not answered. Default value: 30,000 ms.
5. In the **PAMD Fail Time (ms)** field, enter the maximum time to wait for positive answering machine detection or positive voice detection after a cadence break. Default value: 4,000 ms.
6. Click **Apply** to save changes.

Note: The system services must be restarted for the changes to take effect.

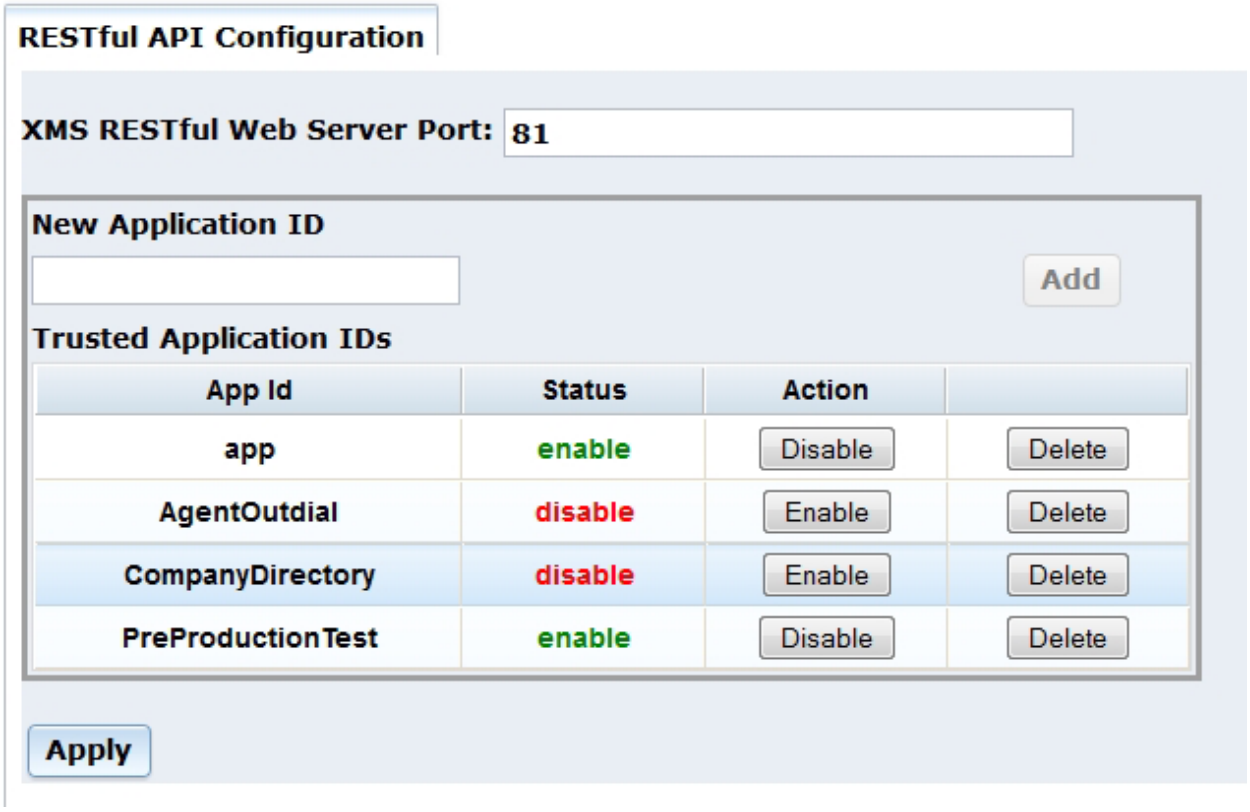
Delete a CPA Configuration

Perform the following steps to delete a CPA configuration:

1. Click in the check box to the left of the CPA configuration you wish to delete.
2. Once you select the CPA configuration, click **Delete**.

RESTful API

The **RESTful API** menu opens to the **RESTful API Configuration** page which is used to configure several aspects of the RESTful call control and media API.



Proceed as follows to configure the **RESTful API Configuration** parameters:

Port

The port number is used by the lighttpd web server, which services the RESTful API.

If the service needs to be run on a port other than the default port 81, this may be configured in the **XMS RESTful Web Server Port** field. Enter the new port and click **Apply**.

Note: The system services must be restarted for the port change to take effect.

Application ID

Application IDs are used in the **Routes** page to map a SIP URL to a specific application. The enabled Application IDs are available from the **Application** drop-down list in the **Routes** page.

To add Application ID, enter name in the **New Application ID** field. Click the **Add** button. The ID will be added to the **Trusted Application IDs** section. The ID will be enabled by default.

It may be disabled but kept in the list by choosing **Disable**. It can be re-enabled by choosing **Enable**. The entry can be entirely removed from the list by choosing **Delete**.

Changes to the list must be activated with **Apply**.

Note: The system services must be restarted for the changes to take effect.

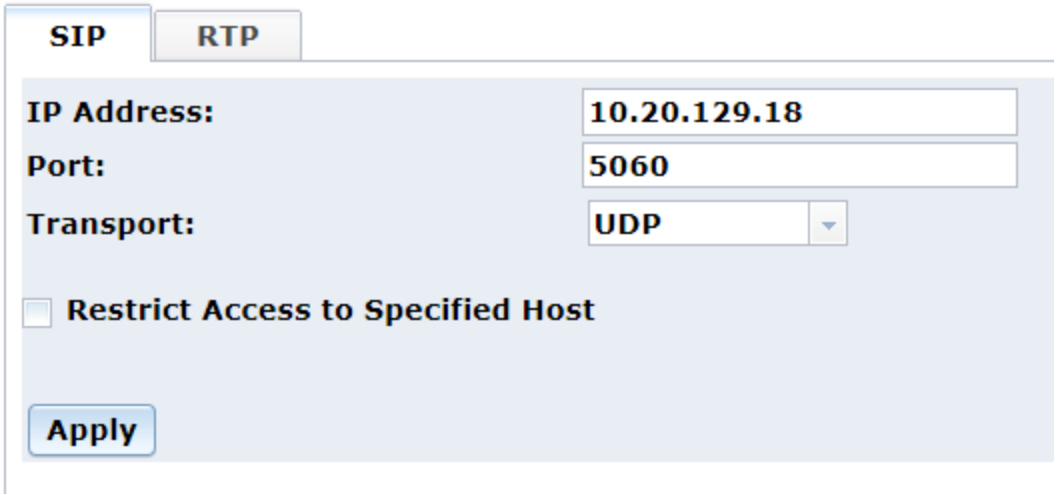
Protocol

The **Protocol** menu contains tabbed pages, **SIP** and **RTP**.

Note: This **Protocol** menu applies to PowerMedia XMS network settings, while the **Network** menu applies to system network settings.

SIP

The **SIP** page is used to configure the **IP Address**, **Port**, or **Transport** information.



The following information is provided:

Item	Description
IP Address	Specifies the SIP IP address. To change the address: 1. Enter the IP address in **IP Address** field. 2. Note the IP address and click **Apply**.

Item	Description
Port	Specifies the SIP listening port. The default is 5060.
Transport	Displays the transport protocol. Two protocols are available from the drop down list: • UDP (User Datagram Protocol) is commonly used for streaming audio and video • UDP_TCP (Transmission Control Protocol)
Restrict Access to Specified Host	Click the check box to restrict access to a specified host.

Changing the SIP IP address is necessary when you have multiple e-net interfaces and want to switch among them, or if you have manually changed the address for the single e-net interface. Refer to the **Network** menu for more information.

Click **Apply** to save changes.

Note: A services restart is required when any changes are made to SIP interface configurations.

Restrict Access to Specified Host

From the **Restrict Access to Specified Host** window, you can restrict access to trusted specified hosts.

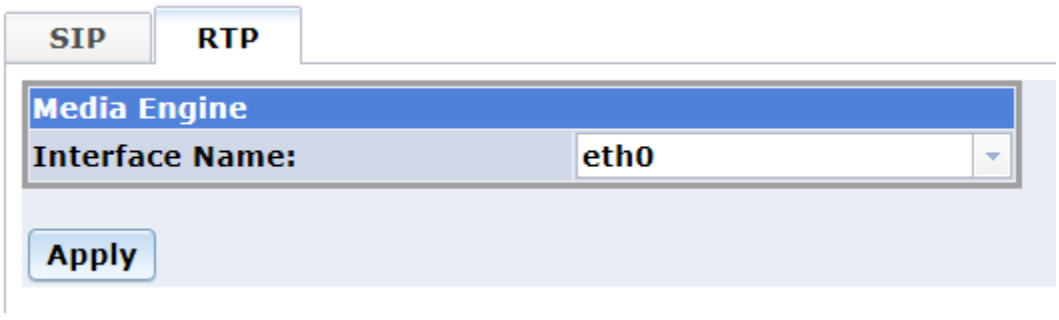
Enter the address you wish to add as a trusted host in the **IP Address** field and click **Add**. The address will be listed in the **Trusted** section.

To delete a trusted host, click on the address listed in the **Trusted** section and click **Delete**.

Click **Apply** to save changes.

RTP

The **RTP** page is used to select the **Interface Name**.

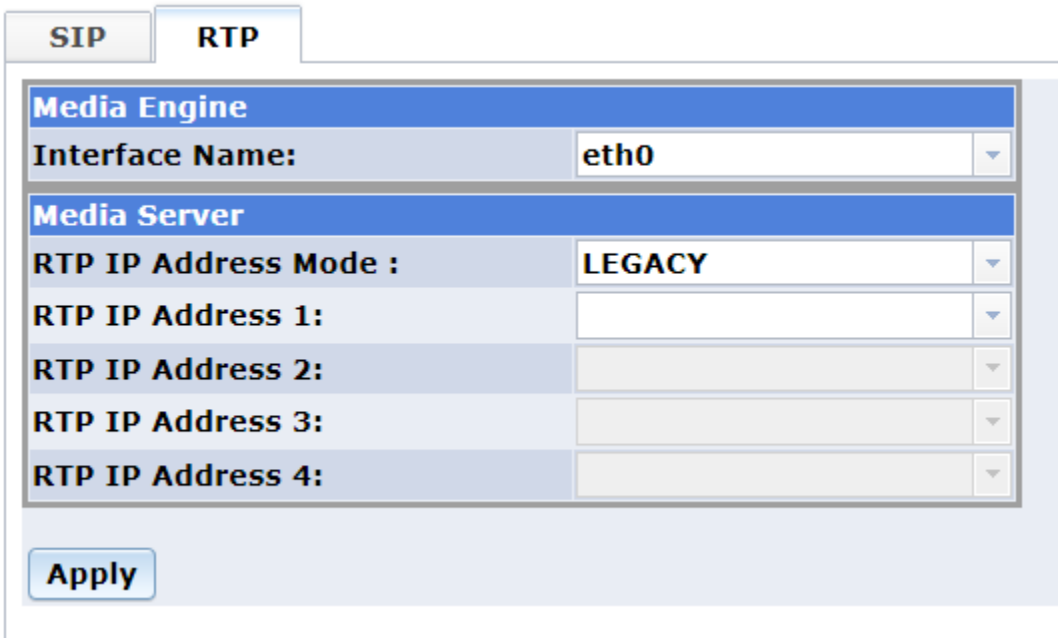


Select the appropriate interface name from the **Interface Name** drop-down list.

Click **Apply** to save changes.

Change RTP IP Address Mode (MSML mode only)

In MSML mode, you can change the **RTP IP Address Mode**.



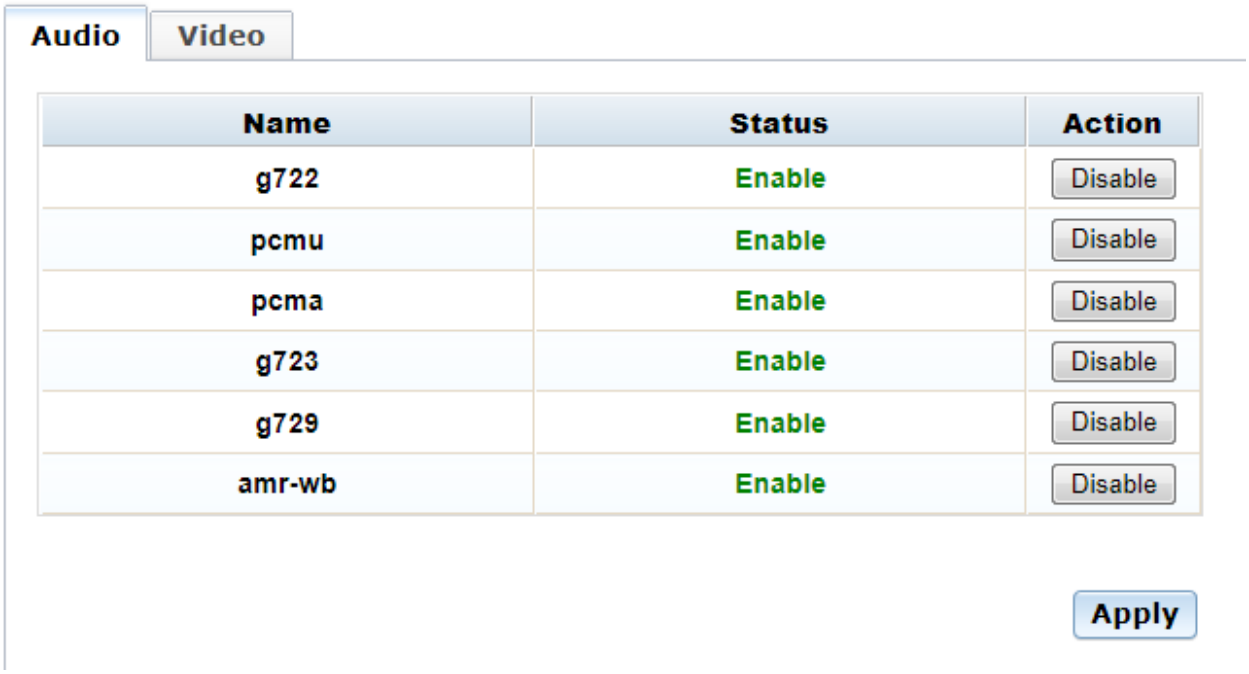
Use the **RTP IP Address Mode** drop-down list to select the value. Valid values are:

- LEGACY (Default value)
  A single RTP IP address should be specified.
- ACTIVE_STANDBY
  Up to two (2) RTP IP addresses should be specified.
- LOAD_BALANCE
  Up to four (4) RTP IP addresses should be specified.

Click **Apply** to save changes.

Codecs

The **Codecs** menu contains tabbed pages, **Audio** and **Video**. On each page, codecs are listed in priority order, with the first row having the highest priority. To change the priority, click on the desired row to select it, and then drag and drop within the table.

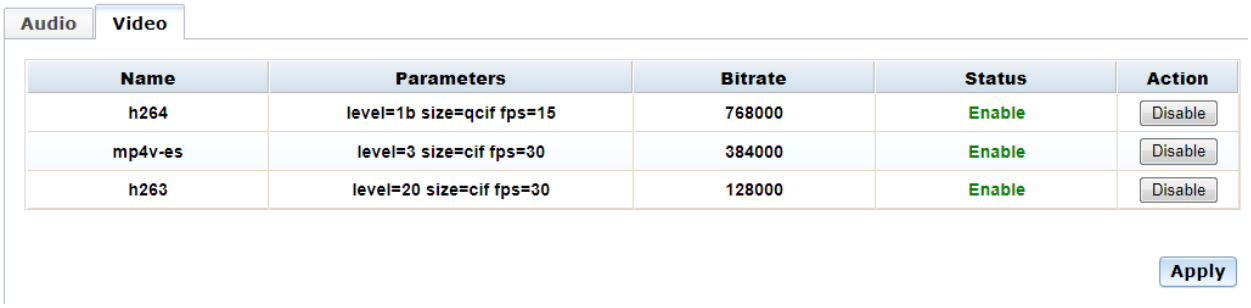


Enable/Disable Codecs

1. Click the button listed in the **Action** column to toggle between **Disable** and **Enable**.
2. Click **Apply** to save changes. The **Status** column will change to the **Action** you selected.

Change Parameters for Video Codecs (MSML mode only)

In MSML mode, you can change the parameters and bitrate settings. Available parameters and bitrates are listed in a drop-down list.



Proceed as follows to configure the **Video** parameters:

Parameters

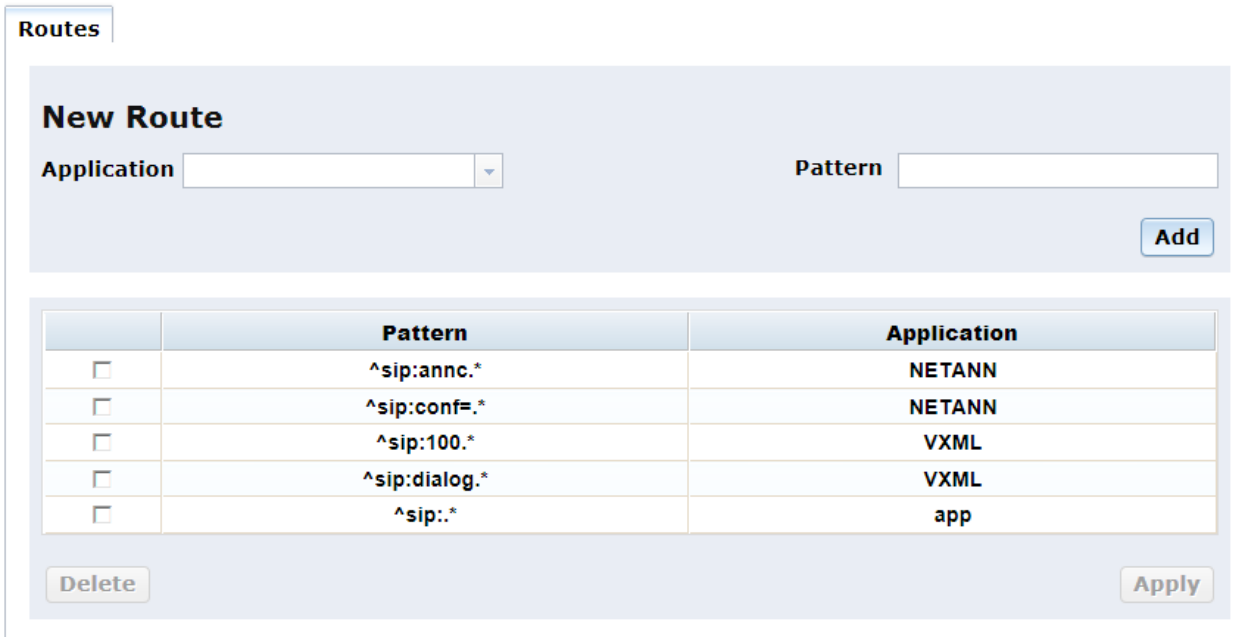
1. Double-click on the appropriate parameter cell in the **Parameters** column.
2. Select the desired parameter from the drop-down list.
3. Click **Apply** to save changes.

Bitrate

1. Double-click on the appropriate cell in the **Bitrate** column.
2. Select the desired bitrate from the drop-down list.
3. Click **Apply** to save changes.

Routing

Accessible in Native mode only, the **Routing** menu opens to the **Routes** page which illustrates how different applications like NETANN, VoiceXML, and RESTful, are engaged with PowerMedia XMS based on the content of SIP URI.



Proceed as follows to configure the **Routes** parameters:

There are two editable fields as part of the **New Route** section on the **Routes** page, **Application** and **Pattern**. Enter new route by clicking **Add** button.

Note: A services restart will automatically be performed once you click **Apply**.

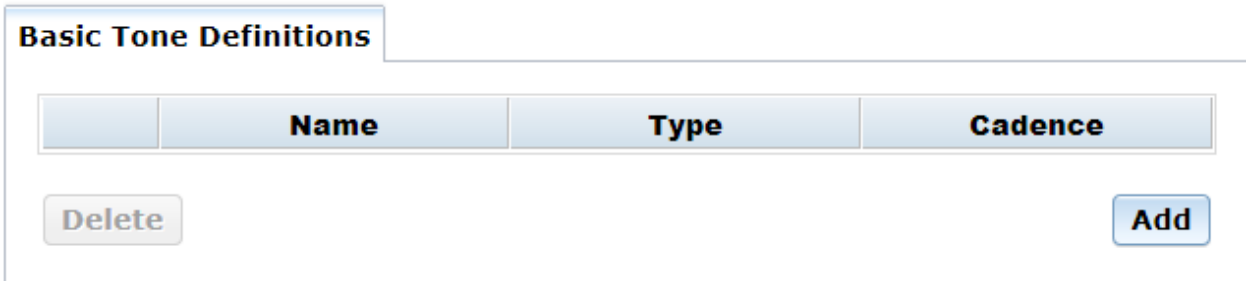
The new route will now be listed on the **Routes** page. Routes can be deleted by clicking in the appropriate check box and clicking the **Delete** button.

Note: The default route for all calls is the application ID "app".

Tones

The **Tones** menu opens to the **Basic Tone Definitions** page which is used to add, modify, and delete tones.

Note: A services restart is required after adding, modifying, or deleting a tone.



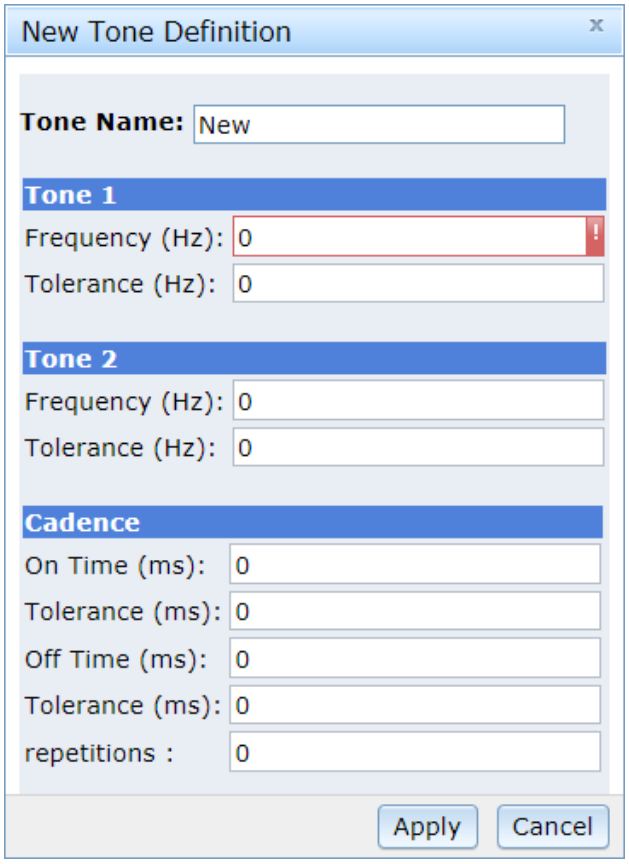
Note: A maximum of 20 tones may be defined.

The following information is provided:

Item	Description
Name	Name of the tone.
Type	Specifies whether tone is a single or dual tone.
Cadence	Specifies cadence. Valid values are: Yes – Cadence tone No – Continuous tone

Add a Tone

1. On the **Basic Tone Definitions** page, click **Add**. The following dialog box appears:



2. Enter the name of new tone in the **Tone Name** section.
3. In the mandatory **Tone 1** field, enter the **Frequency (Hz)**. Frequency range is between 300Hz to 3.5kHz.
4. Enter the **Tolerance (Hz)**. This specifies the deviation in Hz.
5. **Tone 2** field is optional. If only **Tone 1** is defined, then the tone is a single tone. If both **Tone 1** and **Tone 2** are defined, then the tone is a dual tone.

   Note: Dual tones with frequency components closer than approximately 63 Hz cannot be detected. In this case, use a single tone definition.
6. In the **Cadence** section, enter the following in the spaces provided:

   On Times (ms) field: tone-on time in milliseconds (minimum 40 ms). Set to 0 to define a continuous tone.
   Tolerance (ms) field: tone-on time deviation in milliseconds. Cadence only.
   Off Time (ms) field: tone-off time in milliseconds (minimum 40 ms). Cadence only.
   Tolerance (ms) field: tone-off time deviation in milliseconds. Cadence only.
   repetitions field:
7. When finished, click **Apply**.

Modify a Tone

1. On the **Basic Tone Definitions** page, click the check box to the left of the tone you wish to modify.
2. Click on the **Tone Name**.
3. Change the desired fields in accordance with steps 3 through 7 as listed in the procedure to add a tone.

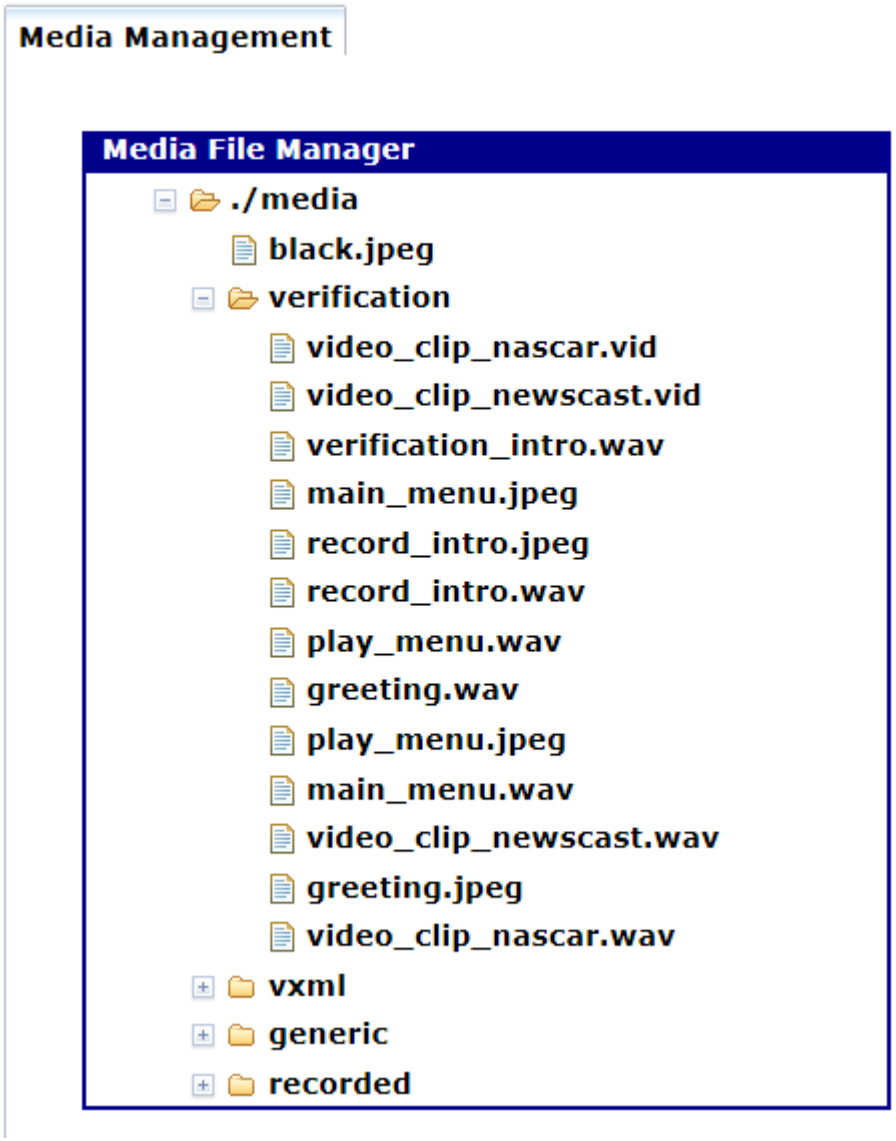
Delete a Tone

1. On the **Basic Tone Definitions** page, click the check box to the left of the tone you wish to delete.
2. Click **Delete**.

Media

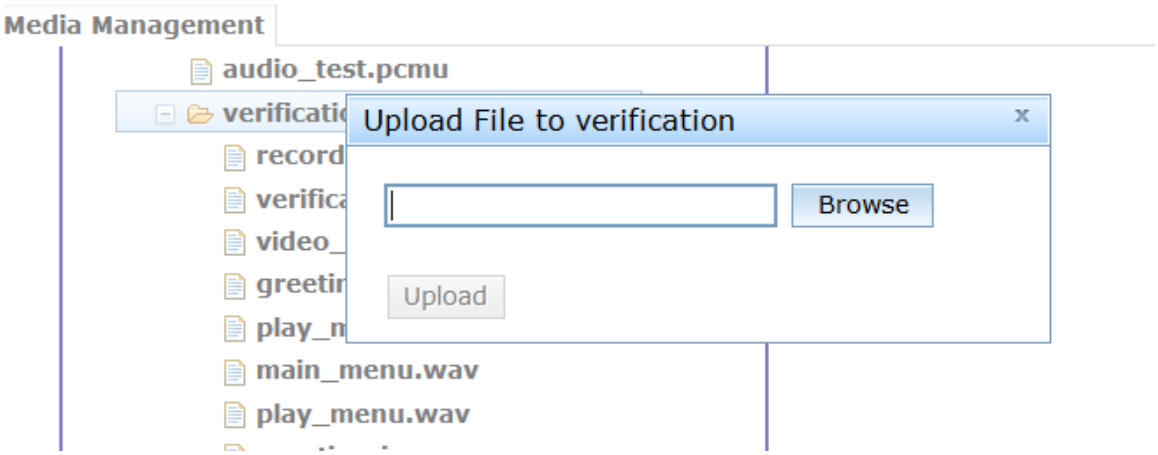
The **Media** menu opens to the **Media Management** page which is used to view and manage the PowerMedia XMS media files. Functionality includes:

- Uploading a Media File
- Deleting a Media File
- Creating a Media File Directory
- Deleting a Media File Directory



Uploading a Media File

1. Select the directory where the downloaded file will reside. For a new directory, see the Creating a Media File Directory section.
2. Right-click and select **Upload Media File**. The **Upload File to verification** dialog box should appear in the vicinity of the selection.



3. Select **Browse** to reach the file explorer. The file explorer look and feel is tied to the operating system of the web browser used.
4. Select a media file that has been downloaded to the system on which your web browser is running. The file explorer will close and the name of the selected file will appear in the text box. Note this text box is read only so to change the file you must click the browser button again and repeat the above steps.
5. Click **Upload** to start the upload process. After a successful upload, the file will appear under the selected directory.

Deleting a Media File

1. Select the file to delete.
2. Right-click and select **Delete**. A delete media file notification dialog will confirm whether to delete media file.
3. Click **OK** to delete the file or click **Cancel** to abort the operation. Upon successful delete completion, the file is removed from the Console's list display.

Creating a Media File Directory

1. Select the parent directory that will contain the new directory.
2. Right-click and select **Create Directory**. The **Enter Directory Name** dialog appears. Enter the name of the directory. To cancel the operation, click **x** in the right top corner of the dialog box.
3. To execute the directory creation after typing the name, press **Enter**. A dialog box is displayed indicating if PowerMedia XMS created the directory.
4. Click **OK**. The new directory will show on the list.

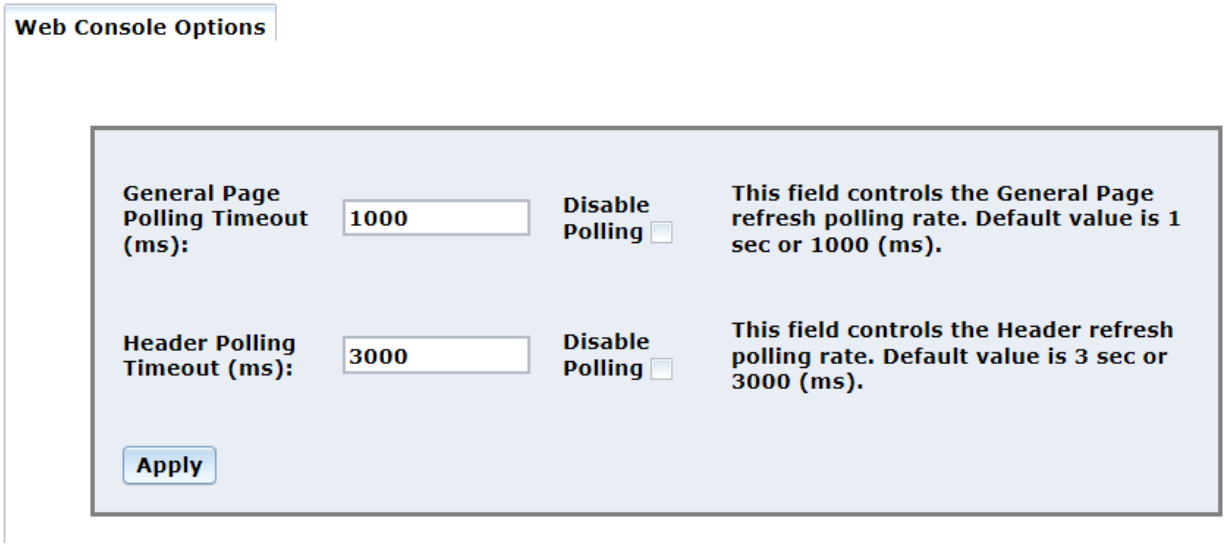
Deleting a Media File Directory

1. Select the directory to delete.

   Note: The root directory (*./media*) cannot be deleted.
2. Right-click and select **Delete**. A delete directory notification dialog will confirm whether to delete the directory and all its contents.
3. Click **OK** to delete the file or click **Cancel** to abort the operation. Upon successful delete completion, the directory is removed from the Console's list display.

Options

The **Options** menu opens to the **Web Console Options** page which is used to configure or disable the Console's polling timeouts.



Proceed as follows to configure the **Web Console Options** parameters:

General Page Polling Timeout (ms)

This value controls the refresh polling rate. The default value is 1 second or 1000 ms. Enter the desired value in the space provided and click **Apply**.

To disable polling, click the check box to the right of **Disable Polling** and then click **Apply**.

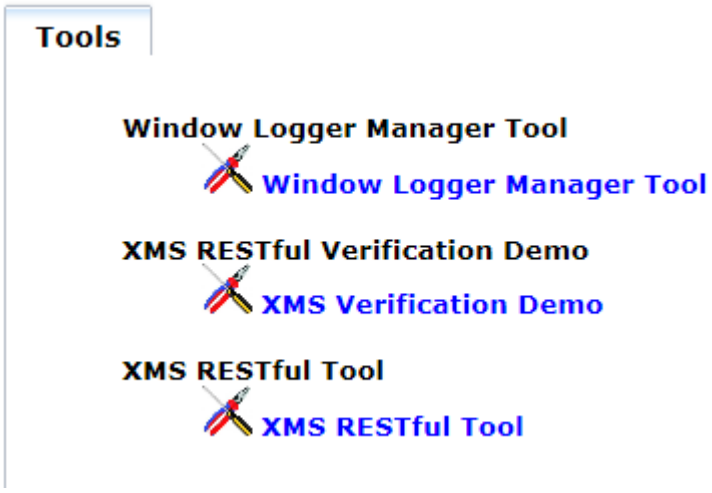
Header Polling Timeout (ms)

This value controls the header refresh polling rate. The default value is 3 seconds or 3000 ms. Enter the desired value in the space provided and click **Apply**.

To disable polling, click the check box to the right of **Disable Polling** and then click **Apply**.

Downloads

The **Downloads** menu opens to the **Tools** page which will be updated periodically as additional demos and tools become available.



The **Tools** page contains the following applications to download:

- **Window Logger Manager Tool**
  Unzips the RemoteRtfTool to your local directory. Refer to the RemoteRtfTool section for more information.
- **XMS RESTful Verification Demo**
  Unzips the XMS Verification Demo to your local directory. Refer to the *Dialogic® PowerMedia™ XMS Quick Start Guide* for more information.
- **XMS RESTful Tool**
  Unzips the XMSTool RESTful Utility. Refer to the XMSTool RESTful Utility section for more information.

To download a file, double-click on the file name and follow the instructions.

Note: Files are downloaded to the local directory you specify.

5. System Level Troubleshooting

Overview of System Level Troubleshooting

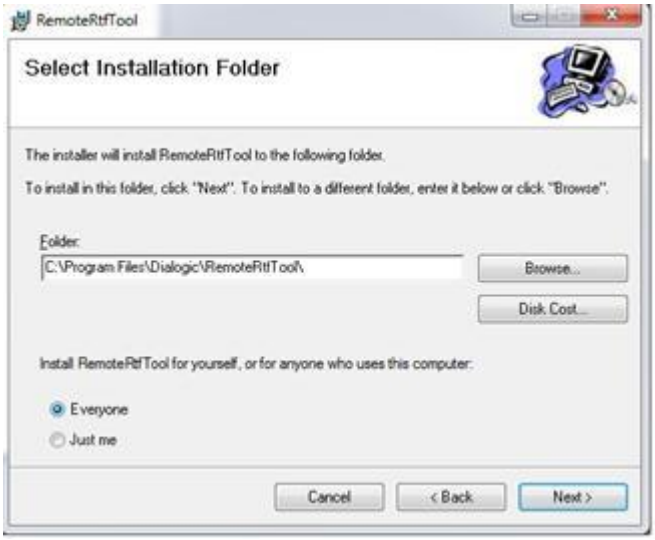
This section provides information about the RemoteRtfTool utility (*RemoteRtfToolInstaller.msi*) and installation log files available to enhance the user experience. It contains the following topics:

- RemoteRtfTool
- PowerMedia XMS Log Files

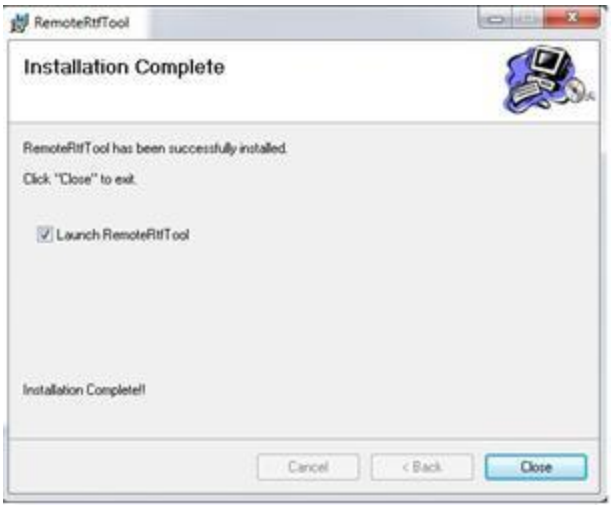
RemoteRtfTool

The RemoteRtfTool utility is provided with the PowerMedia XMS and is accessed through the **Downloads > Tools** page from the Console and double-click *RemoteRtfToolInstaller.msi*.

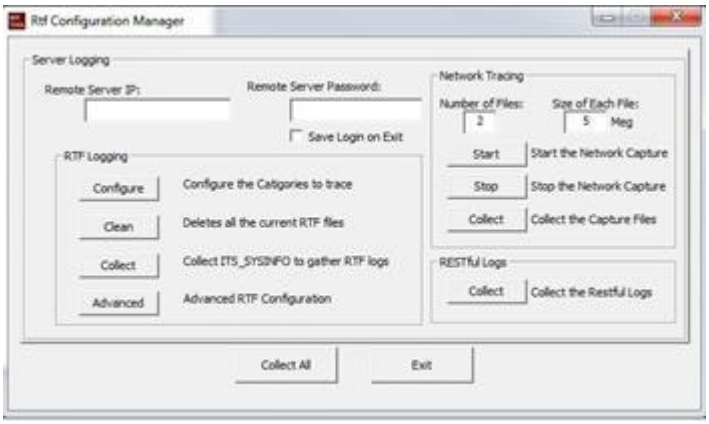
Click **Next**.



Browse to the folder indicated in the screen capture above and click **Next** to start the installation. When the installation is complete, the following screen appears:



The RemoteRtfTool launches and displays the Rtf Configuration Manager window.



Rtf Configuration Manager

The Rtf Configuration Manager contains four sections:

- Server Logging
- RTF Logging
- Network Tracing
- RESTful Logs

Clicking **Collect All** collects all log files in accordance with the default settings of the PowerMedia XMS. Proceed below to change the default settings.

Server Logging

1. Enter the IP address on which to perform the trace in the **Remote Server IP** field.
2. Enter a valid password in the **Remote Server Password** field.

   Notes: The password is not the Console password, but rather the combination used for UserName: root and Password: powermedia.
   For stand-alone RPM installations, password modification is not necessary as the installation script does not change the password to "powermedia" as it does with the .ISO install.
3. Click the check box if you wish to save the login upon exiting the Rtf Configuration Manager.

RTF Logging

The buttons on the RTF Logging section are described below:

Configure

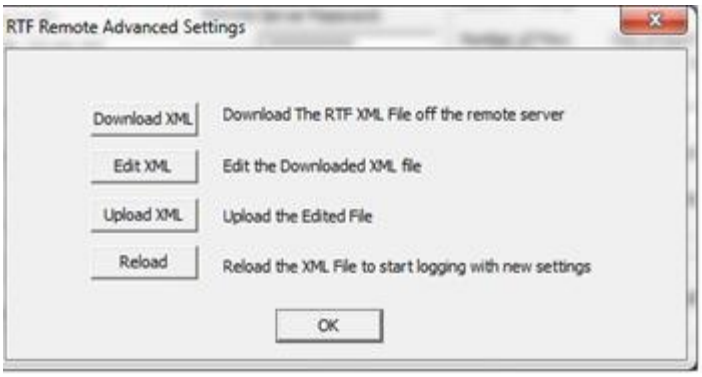
1. Click **Configure** to configure the categories to trace for both Native and MSML modes.

2. In **File Settings**, enter the number of files to trace and the maximum size of each file.
3. In **MSML Categories**, enter the categories you wish to trace.
4. In **Native Categories**, enter the media engine categories you wish to trace.
5. Click **Save** to save configuration settings.

Clean
Deletes the currently stored RTF log files.

Collect
Runs **ItsSysinfo** used to gather RTF log files.

Advanced
Provides the advanced RTF configuration settings.



- **Download XML**
  Downloads the *RtfConfigLinux.xml* file.
- **Edit XML**
  Navigates to the *RtfConfigLinux.xml* file and opens it for editing.
- **Upload XML**
  Uploads the edited file to PowerMedia XMS.
- **Reload**
  Causes the RTF service to reread and restart RTF logging according to the new settings.

Network Tracing

Number of Files
Enter the number of network files to trace.

Size of Each File
Enter the maximum size of each file.

Start
Starts the network capture.

Stop
Stops the network capture.

Collect
Collects the captured files and copies the data to the specified location.

RESTful Logs

Collect
Collects the captured RESTful logs and copies the data to the specified location.

PowerMedia XMS Log Files

The default PowerMedia XMS log location is */var/log/xms*. Consult these log files when troubleshooting specific PowerMedia XMS problems.

Note: Multiple log files are created and capped at 2 MB each.

Retrieving PowerMedia XMS Logs

Most of the PowerMedia XMS logs are not accessible through the Console.

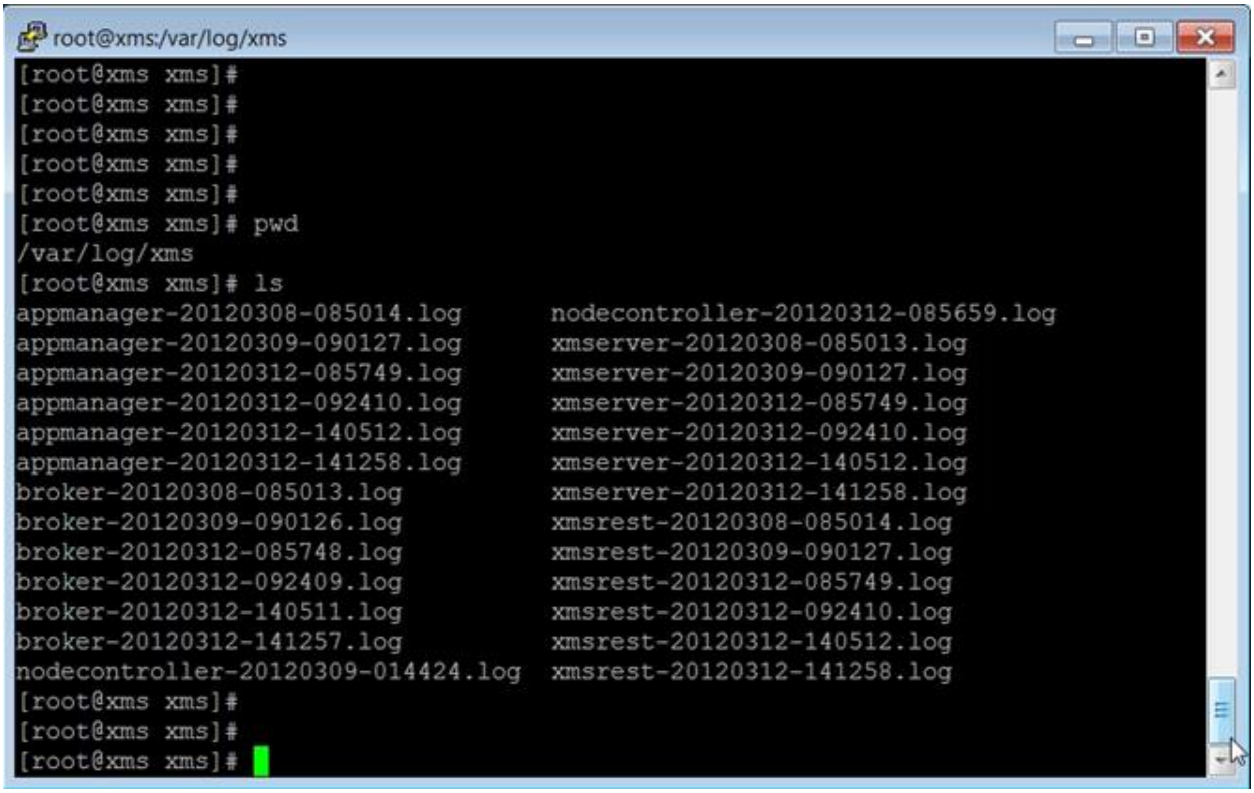
Note: RESTful logs can be collected by choosing "Collect the RESTful Logs" in the RemoteRtfTool utility available for download in the Console.

To retrieve the logs, it is necessary to access the PowerMedia XMS using secure shell (ssh).

The "root" user's default password is "powermedia". If you wish to change the password, do so before proceeding.

Note: For stand-alone RPM installations, password modification is not necessary as the installation script does not change the password to "powermedia" as it does with the .ISO install.

Access the files from */var/log/xms* and copy the logs to the desired location. See the example below:



Log File Retention

The logrotate capability in Linux is used to rotate, compress, and/or mail system log files. It is normally run from cron. It can be configured with the file */etc/logrotate.d/xms* which is specified in the command line when logrotate is run.

The logrotate program deletes any PowerMedia XMS log files older than seven (7) days. To modify this number, access the PowerMedia XMS logrotate configuration file and change the "maxage" field from 7 to the number of days that you wish to retain the logs.

Example

```
/var/log/xms/*.log {
daily
maxage 7
missingok
rotate 0
postrotate
kill -HUP `cat /var/run/nodecontroller.pid`
kill -HUP `cat /var/run/appmanager.pid`
kill -HUP `cat /var/run/broker.pid`
kill -HUP `cat /var/run/xmserver.pid`
kill -HUP `cat /var/run/xmsrest.pid`
endscript
}
```

Contacting Dialogic Technical Services and Support

When reporting an issue to Dialogic Technical Services and Support, be prepared to provide the following information:

- Full description of the issue.
- Version of the PowerMedia XMS software you are using.
- PowerMedia XMS log files.
- Whether the issue is reproducible; the steps that you took.

Note: The latest software update and release notes are available from the Dialogic website at http://www.dialogic.com/support.

6. XMSTool RESTful Utility

Overview of XMSTool RESTful Utility

This section provides details about the XMSTool RESTful Utility (also referred to herein as "XMSTool" or "Utility"). XMSTool is used for developing, debugging, and supporting applications for the PowerMedia XMS using the HTTP RESTful API.

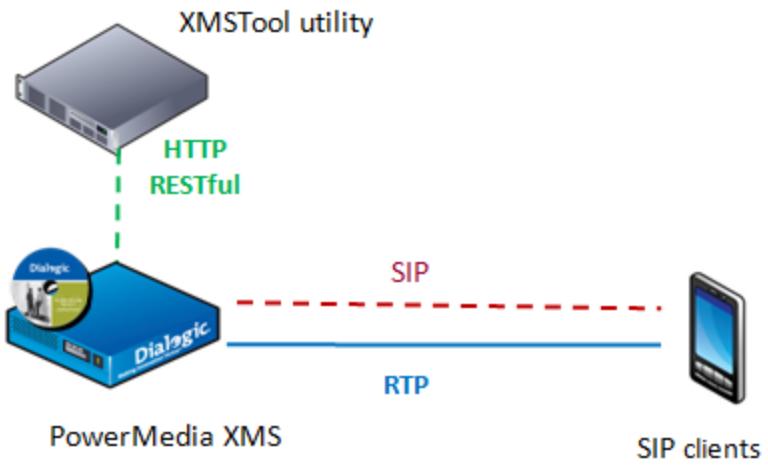
XMSTool is a java-based test application for passing and receiving XMS RESTful API messages to and from the PowerMedia XMS. Supported for both 1PCC and 3PCC (see the Call Control Models), it can be used to build and parse individual RESTful messages, and can drive and record simple applications. The utility provides the following:

- Ability to manually enter and execute the XMS RESTful API commands and observe the results
- Pre-recorded Macros available for commonly used call scenarios
- Method to record Macros for automated execution of command sequences (Demo mode), enabling users to create simple Demos and debug their applications
- Logging capabilities

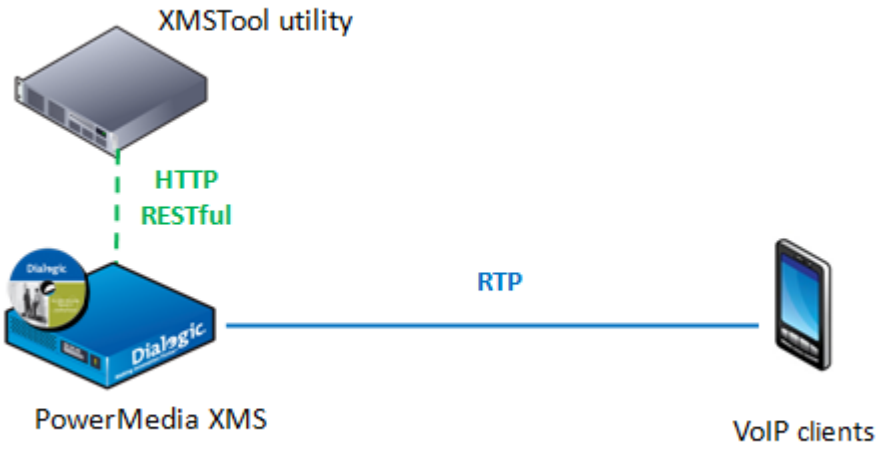
Call Control Models

XMSTool can establish media connections on both 1PCC and 3PCC modes.

With the 1PCC model, illustrated below, the PowerMedia XMS handles inbound and outbound SIP calls, taking advantage of its built-in SIP call control functionality. XMSTool controls all aspects of the PowerMedia XMS operation, including SIP call control.



With the 3PCC model, illustrated below, the XMSTool only directs the PowerMedia XMS to establish and manipulate the RTP-based media sessions. This model is commonly used in VoIP network environments such as IMS, where SIP call control is performed by an application server. This model permits using signaling protocols other than SIP and allows application architects the flexibility of choosing the signaling protocol.



Prerequisites

Prior to using XMSTool, the user is expected to:

- Understand the functionality and operation of the PowerMedia XMS.
- Be familiar with the HTTP RESTful control interface of the PowerMedia XMS in order to use the tool in Demo mode.
- Understand the HTTP RESTful interface of the PowerMedia XMS and have a working knowledge of XML and related topics (data structures, XSD, etc.) in order to use the tool at the individual command level (Advanced mode).
- Understand the key concepts of a service-oriented architecture and HTTP RESTful interface.
- Have a working knowledge of Java programming.

Starting XMSTool

XMSTool is written in Java, making it operating system independent. The PowerMedia XMS on which it runs requires a Java Runtime Environment (JRE). The version of Java Standard Edition (JSE) used for the tests described in this document is Version 7, Update 2, build 1.7.0_02-b13.

Before starting XMSTool, be sure that the PowerMedia XMS itself is running and in Native (RESTful) mode. A SIP softphone should also be available. See the *Dialogic® PowerMedia™ XMS Quick Start Guide* for information about setting up PowerMedia XMS and installing suitable SIP softphones.

Download XMSTool using the Console. From the **Downloads > Tools** page, choose the **XMS RESTful Tool**. Unzip the downloaded distribution and then go to the top level directory where you will see the /dist and /testing directories. From the top level directory, run the tools as follows:

```
> java -jar dist/XMSTool.jar -g -m <xms_server_ip_address>
```

Note: XMSTool can be run to expose its graphical user interface (GUI) or as a command line interface. Using the GUI provides access to both modes – Demo/Simple and Advanced. Running from the CLI only allows Demo/Simple mode.

XMSTool Utility Modes

XMSTool can be run in two different modes:

- Demo/Simple Mode
  Uses predefined XML scripts; short application scenarios can be executed to demonstrate most of the PowerMedia XMS RESTful functionality. Session logging is available to examine the message interchange. Only sessions using inbound SIP calls are currently available in this mode.
- Advanced Mode
  Allows individual RESTful commands to be manually entered for full PowerMedia XMS control. This mode is intended to be used by developers who are looking to become familiar with the RESTful API messages used to control PowerMedia XMS. It also allows the individual commands that make up a macro/demo to be recorded for replay or to provide an accurate way to reproduce a problem in PowerMedia XMS.

Demo/Simple Mode

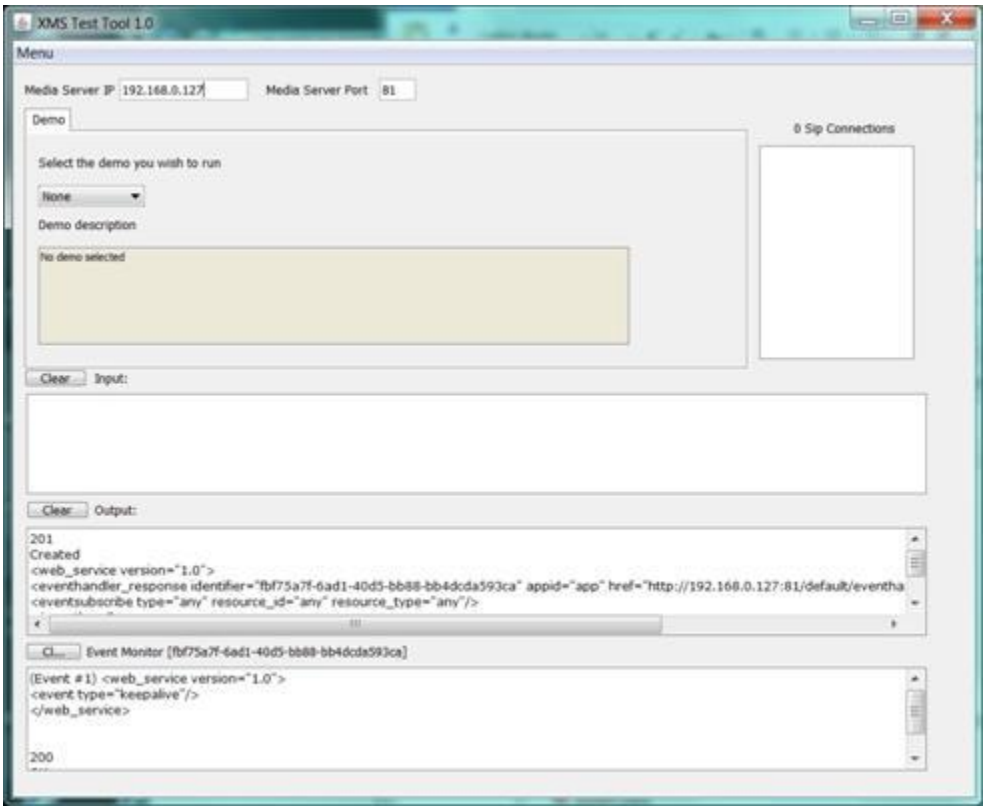
In this mode, XMSTool is used to execute predefined demos or macros that string together a series of RESTful request and response messages to make up a simple application, such as answering a call and playing a file or putting a caller into a video conference.

The **Demo** screen provides access to the demos listed below.

Note: All demos are multimedia – both audio and video.

- **Play**
  Answers an inbound call and plays a file.
- **Collect**
  Answers an inbound call (audio only) and collects four (4) digits. When the 4th digit is entered, the digit collection event is seen in the event handler window. The call will be automatically disconnected several seconds after the digit event is returned.
- **Join**
  Joins two inbound callers into a conference. The callers remain connected for ten (10) seconds, and then the conference is torn down.
- **Conference**
  Joins a single inbound caller into a conference. The caller remains connected for eight (8) seconds, and then the conference is torn down.

- **Confplay**
  Joins two inbound callers into a conference and a file is played. After the play terminates, the conference is torn down.
- **Record**
  An inbound caller is prompted by a file. After the prompt is played, record mode is entered. The recording can be terminated with # or ends by itself after ten (10) seconds.



Proceed as follows to run a demo:

1. Select a **Demo** from the drop-down list.
2. Place an inbound call from a SIP softphone. Any SIP user name (or extension) may be used with XMSTool, as the scenario selection is done through the drop-down list.
3. Make a call to the IP address of the PowerMedia XMS. The call will be answered by PowerMedia XMS and XMSTool, and the appropriate scenario will be played.

   Note: Several scenarios will use two callers.

Details about the application's call flow may be found in the XMSTool's session log, which is located in the testing directory and named *xmstool.log*. The logger overwrites the log file each time XMSTool starts.

Note: All demo scenarios start when an inbound call is received. Currently, outbound calls cannot be used.

Accessing XMSTool using CLI

Demos are also accessed through the command line interpreter (CLI) when a windowing system on the host computer is not available.

Proceed as follows to use the CLI interface:

1. Start the tool from the operating system command prompt:

```
> java –jar dist/XMSTool.jar –r –m <xms_server_ip_address>
```

2. Upon successful connection to PowerMedia XMS, all available test scenarios for inbound calls are displayed:

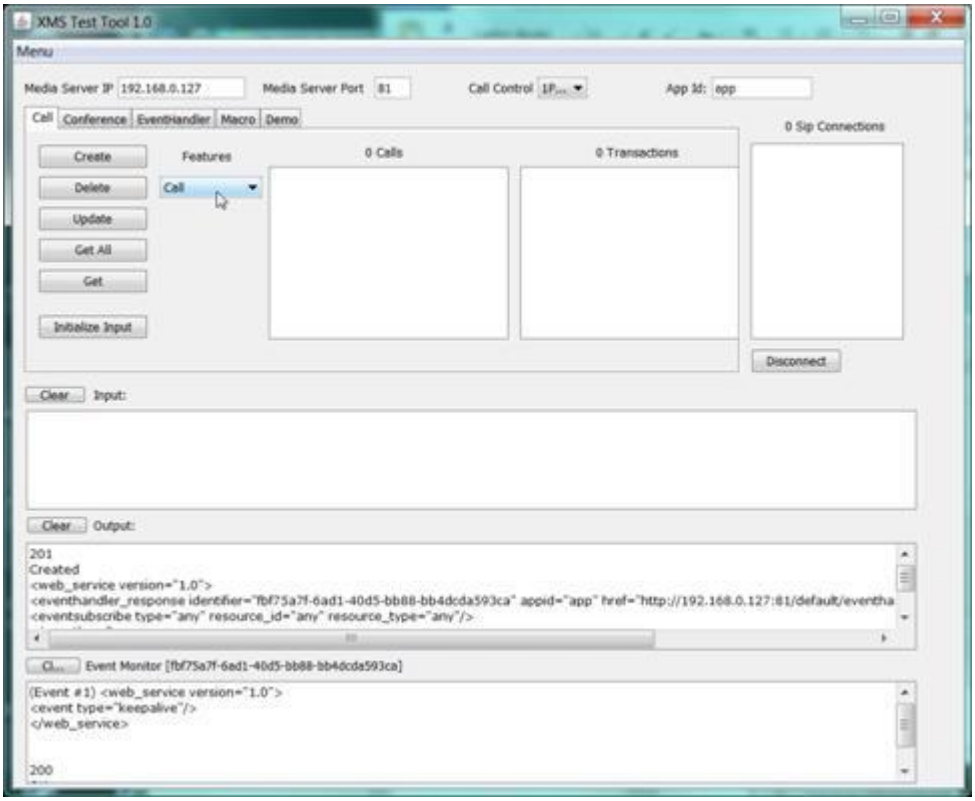
```
XMSTool Application
-------------------
Demos
-----

[collect]
Description: Play and collect demo

[conference]
Description: 2 party 10 second conference demo

[confplay]
Description: 2 party conference play demo

[join]
Description: Join 2 calls for 10 seconds demo

[play]
Description: Play demo

[record]
Description: Record demo

Waiting for incoming calls ...

XMSTool>
```

3. Access a scenario by placing a SIP video call to the IP address of PowerMedia XMS using the test name as the SIP user name. For example, entering Sip:play@192.168.1.100 will connect to the PowerMedia XMS at IP address 192.168.1.100 and execute the multimedia file "play" test scenario.
4. Stop XMSTool using the exit command at the CLI prompt.

Advanced Mode

Advanced users and RESTful application developers may choose to enter individual commands to closely examine the RESTful messages used. This method is useful when designing and coding one's own RESTful applications.

To accomplish this, select **Advanced** mode from the **Menu** drop-down list using **Menu > Advanced Mode**. The following window appears:



The following existing connection and operation parameters are displayed:

- **PowerMedia XMS IP**
  Display only, set with XMSTool command line startup -m option.
- **PowerMedia XMS Port**
  Display only, set with XMSTool command line startup -p option.
- **Call Control**
  Specifies protocol used.
- **App Id**
  Specifies the PowerMedia XMS application to connect to. Corresponds to an application set on the **Routing > Routes** page from the Console. Defaults to "app".

The **Call**, **Conference**, **EventHandler**, **Macro**, and **Demo** tabs pertain to the different modes and messages used by XMSTool, while the **Create**, **Delete**, **Update**, **Get All**, and **Get** buttons determine the HTTP methods (GET, POST, PUT, DELETE) used to send the RESTful messages.

The **Features** drop-down list is used to select the media and call actions that make up the application flow. The **Calls**, **Transactions**, and **SIP Connections** areas list the IDs of all active calls, media transactions and SIP connections.

The three large horizontal text windows are used for building the XML input to PowerMedia XMS, for displaying responses from PowerMedia XMS to RESTful messages that have been sent, and for displaying events sent from the event handler in PowerMedia XMS.

When XMSTool starts, the event handler is created to relay unsolicited events to the XMSTool client. An Event Monitor ID is seen on the top of the lowest window. All content is cleared using the **Clear** button.

Individual commands, such as **Create**, are sent in a specific sequence for successful operation. The following table explains the sequences.

Sequence	Tasks
Create	1. Select either a **Call** feature from the **Call** tab or a **Conference Feature** from the **Conference** tab. 2. Click **Initialize Input** to initialize the command and clear any existing content. 3. Edit, if necessary, the default command. For example, max_parties for a conference defaults to 2 and may need to be increased, or the destination URI for an outbound SIP call may need to be adjusted. 4. Click **Create** to generate an HTTP POST containing the RESTful command issued. Responses to commands are displayed in the Output window.
Update	1. Select the entity (call, conference or transaction) ID. (For example, issuing a Stop command on a Play operation only requires selecting the Play transaction ID. Adding a party to a conference requires two ID selections, the Call ID and the Conference ID.) 2. Click **Initialize Input** to clear any existing input and update with the default XML used with the command. 3. Edit the RESTful commands as desired. For example, change the file to play in a Play operation. 4. Click **Update** to generate an HTTP PUT that contains the new RESTful command. Responses to commands are displayed in the Output window.
Get All and Get	1. Select either the **Call** tab or **Conference** tab to access existing calls or existing conferences. 2. Click **Get All** to generate an HTTP GET which returns information on all calls or all conferences depending on the tab selected. 3. For specific call or conference information, click **Get** to generate an HTTP GET. Information returned is displayed in the Output window.

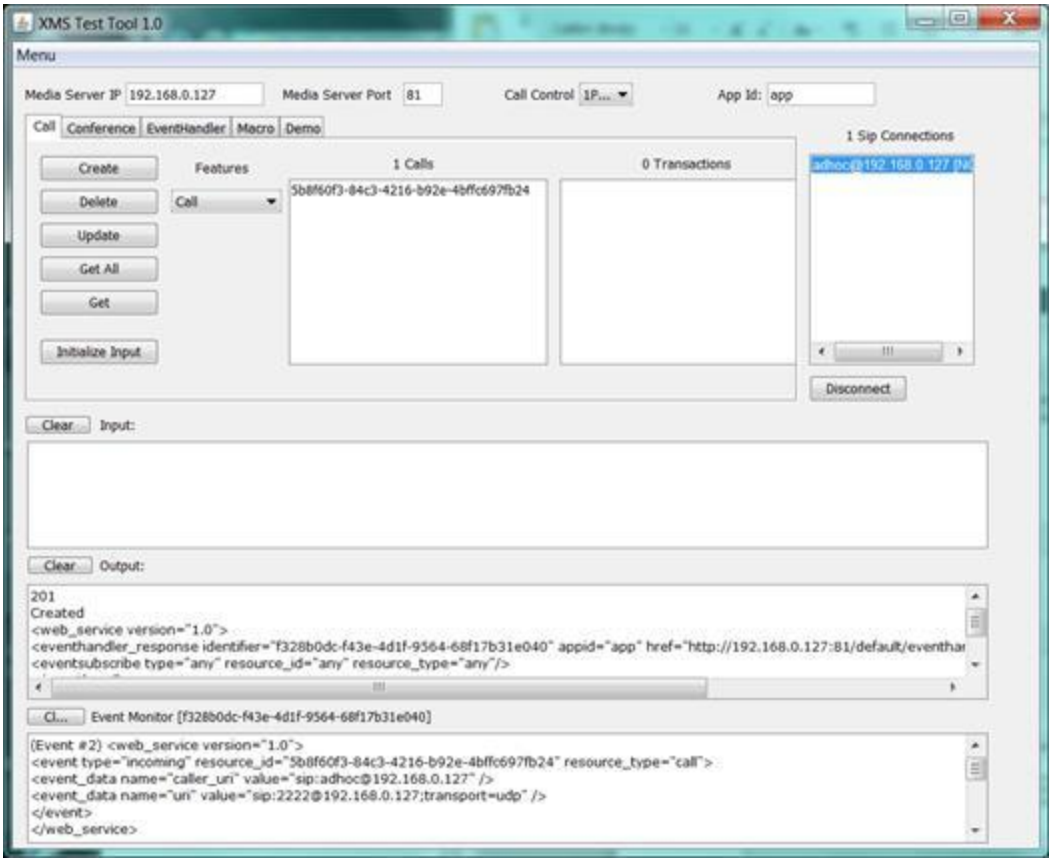
Sequence	Tasks
Delete	1. Select the ID of the Call or Conference. 2. Click **Delete** to generate an HTTP DELETE for the selected entity. A 200-series OK reply with no content will be displayed in the Output window.

Basic Operation and Commands

The following sections provide examples of basic commands.

Receiving an Inbound Call

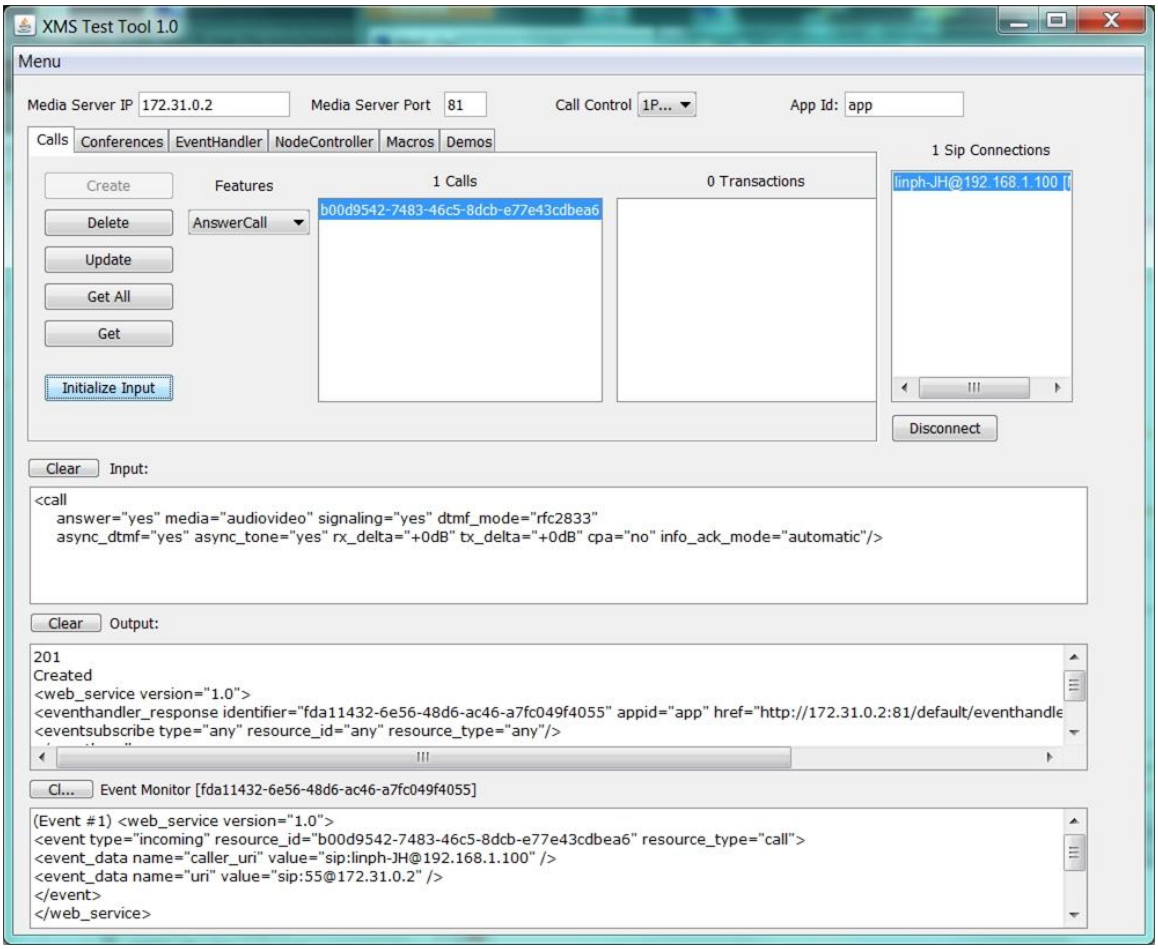
The **Call** tab is used to handle setup and teardown of a call. Inbound calls require a SIP softphone to initiate the call using any SIP user name (or extension). When a call is made to the IP address of the PowerMedia XMS, notification of the call is sent to XMSTool and displayed in the Input window as shown below:



The call offered event ("incoming") can be observed in the Event Monitor window. Proceed as follows to reply to the event:

1. In the **Call** tab, select the ID of the received call.
2. Select **AnswerCall** from the **Features** drop-down list. Alternately, **AcceptCall** could be selected if, for example, early media were desired. This would allow a file to be played to the caller before the call is answered.

3. Click **Initialize Input** to create a reply to the call offered event.
   The answer message will be automatically generated. Note that the default values set in the message may be edited if desired.



4. Click **Update** to send the answer message.
   The connection to the SIP softphone is now established.

Making an Outbound Call

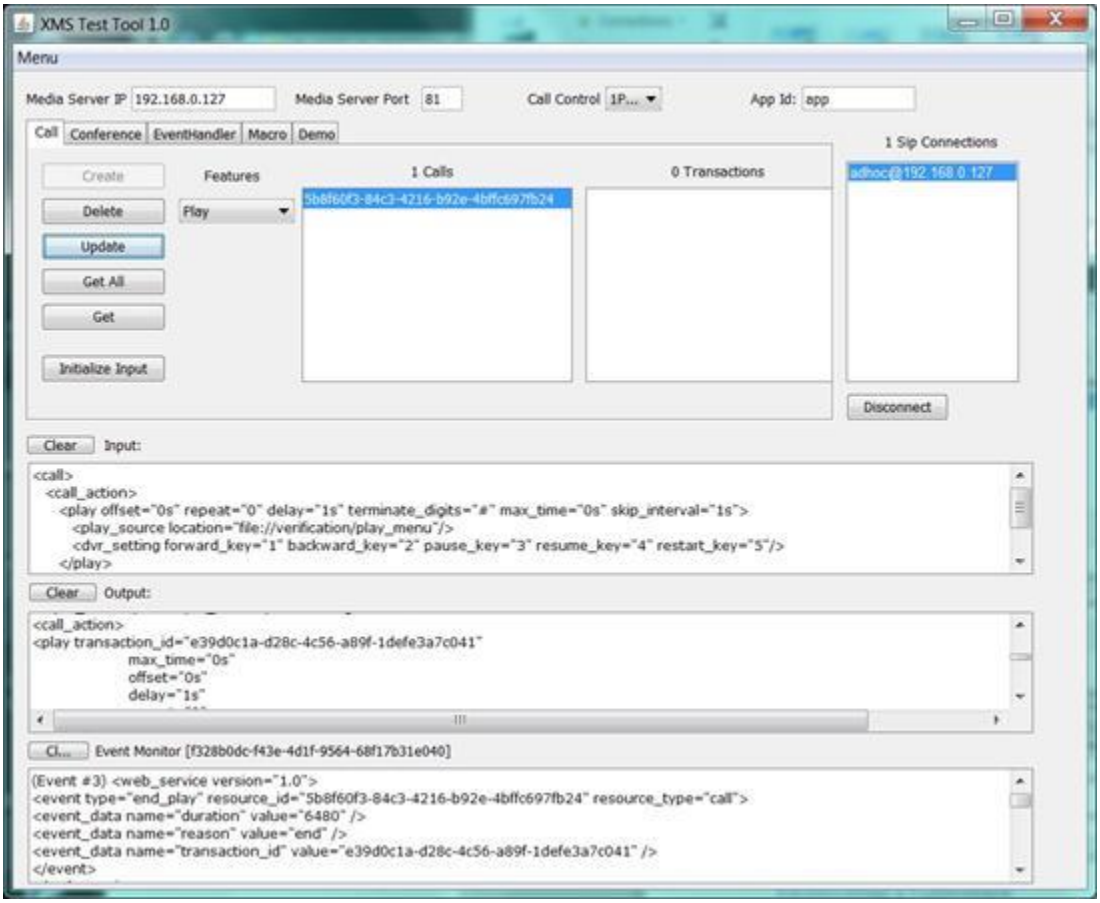
The **Call** tab is used to handle outbound call setup and teardown. The SIP softphone to call should be set in a mode where it can detect incoming calls and either ring or automatically answer them.

1. Click **Initialize Input** to generate a RESTful Call command.
2. Edit the default command. For example, the destination_uri and source_uri should reflect the SIP address of the SIP softphone being called and the PowerMedia XMS, respectively. Other default values may be adjusted if desired.
3. Click **Create** to launch the call.
   The SIP softphone will ring and the call is connected when answered.

Playing a File into a Call

Once a call is connected, media commands may be issued. In the following example, a multimedia file is played.

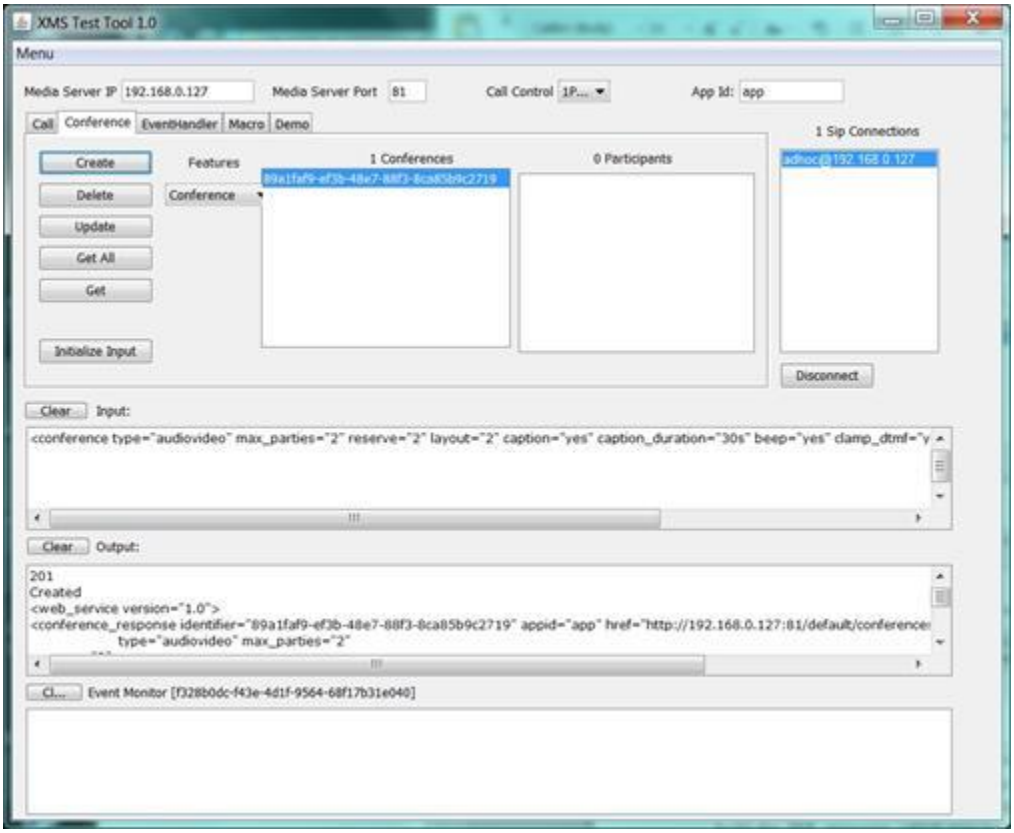
1. Select the call ID.
2. Select **Play** from the **Features** drop-down list.
3. Click **Initialize Input** to provide a call action command to play a file.
   Although a default file and default parameters are provided, these may be edited before being sent.
4. Click **Update** to send the message.
   If successful, the audio/video is heard/seen on the SIP softphone. The response to the play command is displayed in the Output window when the play is initiated, and a play termination event seen in the Event Monitor window once the play is complete.



Establishing a Conference

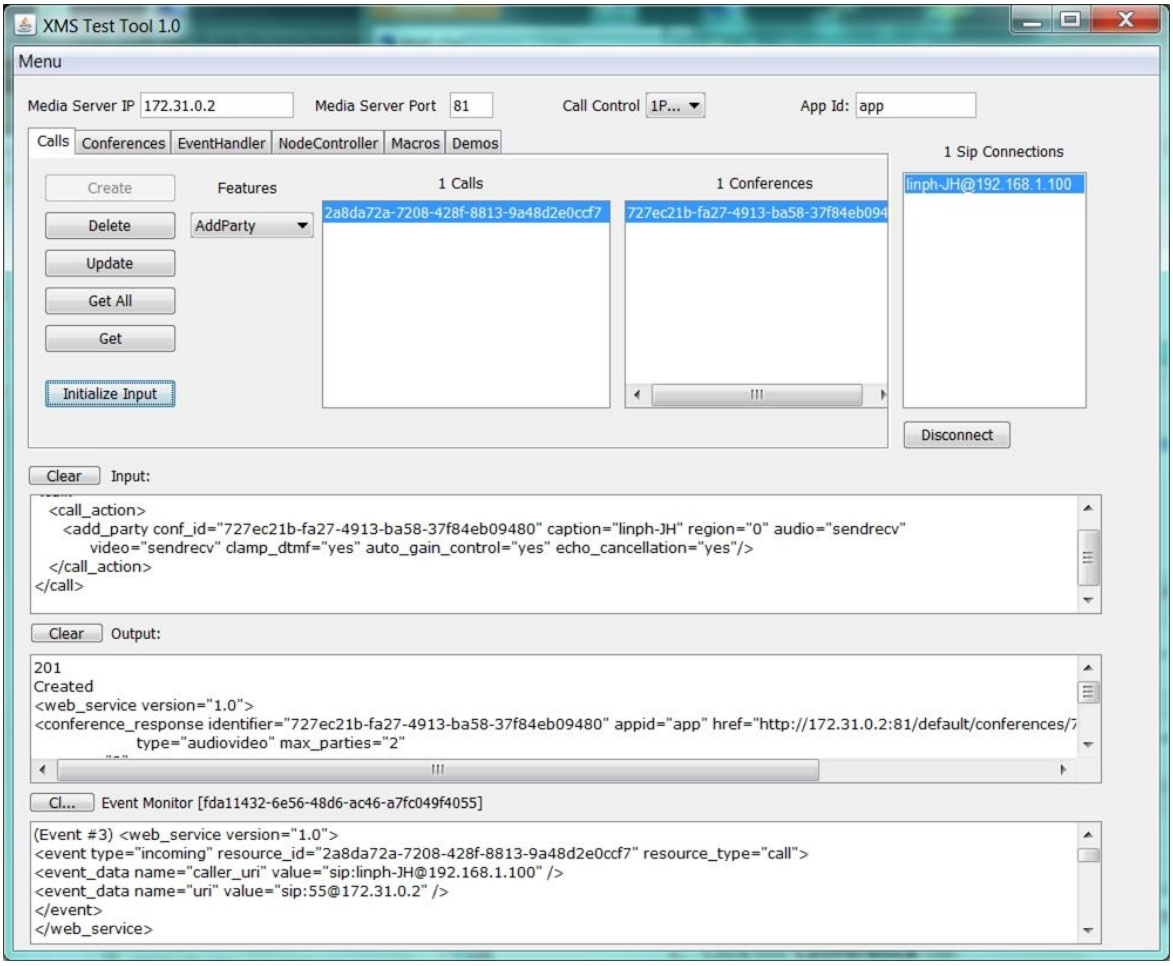
Once a call is idle, a video conference may be started. First, create a conference in which to add the call.

1. Click the **Conference** tab.
2. Click **Initialize Input** to get the default conference creation parameters. Edit them if desired.
3. Click **Create** to establish the conference and generate a conference ID.



4. Click the **Call** tab.
5. Select the call ID and the ID of the conference just created.
6. Select **AddParty** from the **Features** drop-down list.
7. Click **Initialize Input** to build the XML message, which may be edited as desired.
8. Click **Update** to add the caller to the conference.
   The SIP caller will be in a single-person conference.

For a multi-party conference, make additional calls and add each to the conference using the above procedure.



The conference may be torn down and cleaned up in the following order:

1. Click the **Conference** tab.
2. Select the call ID and click **RemoveParty** from the **Features** drop-down list. Repeat for each party in the conference.
3. Select the call ID and click **Disconnect** for each party in the conference.
4. Select the conference ID and click **Delete**.

Additional XMSTool Commands

Many additional XMS RESTful commands can be run using XMSTool. Listed below are all available call actions. For the complete list of commands and their parameters, refer to the *Dialogic® PowerMedia™ XMS RESTful API Developer's Guide*.

The following call actions are available from the **Features** drop-down list in the **Call** tab. In most cases default values can be used, but it is good practice to check the parameters before applying. For all commands, the call ID must be selected before clicking **Initialize Input**.

Command	Description
AcceptCall	Accept an offered call, but do not yet answer it. This command is desirable for early media or to redirect a call elsewhere.
AnswerCall	Answer an offered call.
PlayCollect	Play a multimedia file and collect DTMF digit(s) during the play. The default message is set to collect four (4) digits. The result of the digit collect operation will be displayed in the Event Monitor window.
PlayRecord	Play an introductory multimedia file and then record it. Default recording termination is either the # key or a maximum time (10 seconds). The resulting file, "recorded_file", is played back using the Play command and setting play_source location=file://recorded_file.
Overlay	Display an image overlay on the active call.
Join/Unjoin	Used to bridge or un-bridge two active calls.
Addparty/ Updateparty/ Removeparty	Used to add, modify, or remove a call from an existing conference. It may be necessary to change the default add and update options for this command. **Note:** A conference must be created before adding a party.
SendDTMF	Send the specified DTMF tones to the connected call.
SendINFO	Send a SIP INFO message to the caller.
SendInfoAck	Manually acknowledge a SIP INFO message received from the caller.
Transfer	Transfer (attended or unattended) the caller to the specified SIP URI.
Redirect	Redirect an accepted but unanswered call to the specified SIP URI.
Hangup	Send a SIP BYE message with the specified content to hang up the call. This is the equivalent of hanging up using the HTTP DELETE method, but allows a message to be sent along with the BYE.

The following call actions affecting an ongoing conference are available from the **Features** drop-down list on the **Conference** tab. For all commands, the call ID must be selected before clicking **Initialize Input**.

Command	Description
Play	Play a file into an ongoing conference. The video will appear as an overlay to the entire conference.
UpdatePlay	Change the play characteristics of the ongoing play file in the conference.
Stop	Stop playing a file in an ongoing conference and return the conference to the participants.

Note: The **Disconnect** button under the SIP Connections window sends a DELETE to the proper call ID to hang up the call, making it easier for the user to know which call they disconnected. This feature specifies which call ID corresponds to which incoming SIP call.

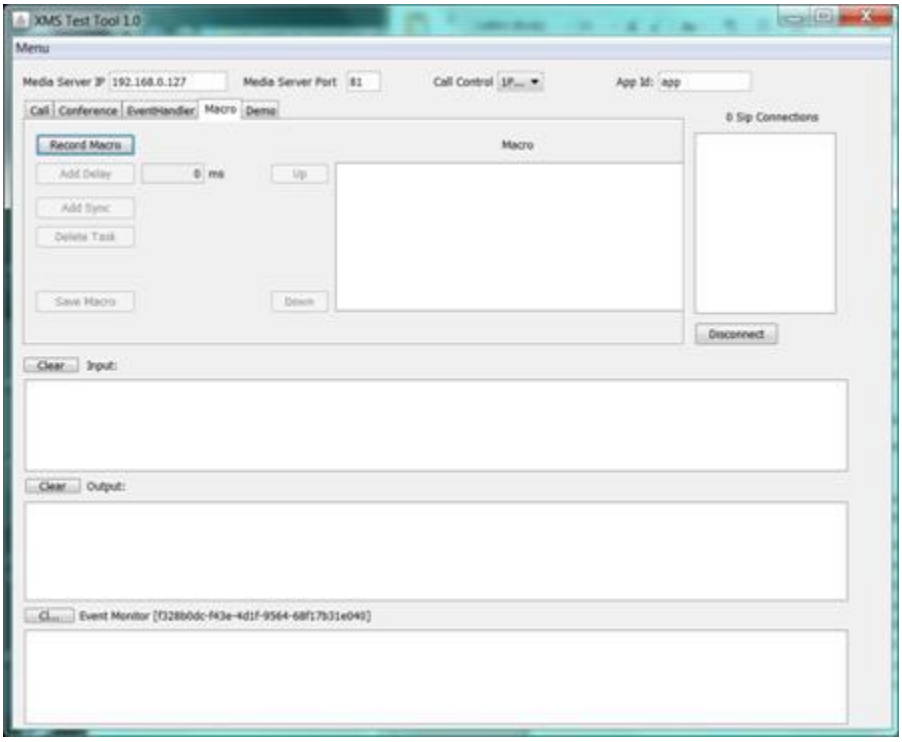
Using XMSTool to Record Macros/Demos

XMSTool has the ability to record a sequence of commands for an application scenario for later use. The recording can be saved and will appear in the installation's Demo directory.

Note: Macros are saved in XML format in the */testing* directory under *macro_name.xml* file.

Prior to recording a Macro, be sure that XMSTool is completely idle and that no Demos are running. To see Demo status, click the **Demo** tab and verify that none are listed in the Demo box.

To start a recording, select the **Macro** tab and click **Record Macro**. The following window displays:



Note: Macro recording begins when an inbound call is received. Currently, outbound calls cannot be used with **Record Macro**, either at the start of the macro or within it.

When an inbound call arrives, individual commands may be accomplished until the application scenario is complete. Since all manual commands, even erroneous ones, are logged, it is suggested that a scenario be run several times with no error responses before clicking **Record Macro**. To stop recording, click **Stop Macro**.

The **Add Delay** button is provided for timing an indeterminate command, such as a conference for a given number of seconds, before moving on to the next command. Add a delay by clicking **Add Delay** and setting a value in milliseconds.

Note: Many RESTful commands have a time parameter.

The **Add Sync** button is provided to sync the actions of all participants involved in either the same conference or joined call. This option verifies that all inbound calls have arrived before continuing with a macro. Callers are grouped together using their SIP "FROM" user name. For example, if six callers all have the same SIP From username and the executing macro has a <Sync> command, that macro waits until all other callers in that group are at that point before continuing.

The **Delete Task** button is used when an erroneous command is identified. The line containing the command may be deleted by selecting the entire line and clicking **Delete Task**.

Tasks can be ordered differently using the "Up" and "Down" buttons next to the **Macro** box.

When satisfied with the recording, name the file and click **Save Macro**. The file is now written into an XML file in the */testing* directory and will be available in the **Demo** list for replay.

Note: The name of the recording must be manually added to the */testing* directory under *xmstool.cfg* file if the macro is desired when XMSTool is restarted.